# CRITICAL ISSUES IN ROBOT-HUMAN OPERATIONS DURING THE EARLY PHASES OF THE SPACE STATION PROGRAM

A COOPERATIVE PROJECT OF

AUBURN UNIVERSITY

RENSSELAER POLYTECHNIC INSTITUTE

UNIVERSITY OF MICHIGAN

UNIVERSITY OF TEXAS AT ARLINGTON

ORGANIZED BY THE
CONSORTIUM FOR SPACE/TERRESTRIAL AUTOMATION AND ROBOTICS
A DIVISION OF
UNIVERSITIES SPACE RESEARCH ASSOCIATION

C-STAR INTERIM HEADQUARTERS
CALIFORNIA SPACE INSTITUTE
M.S. A-016
UNIVERSITY OF CALIFORNIA, SAN DIEGO
LA JOLLA, CA 92093-0216

WORK PERFORMED UNDER
NASA GRANT NAG 5-939

FOR
GODDARD SPACE FLIGHT CENTER
SPACE STATION
FLIGHT PROJECTS DIRECTORATE

DR. JAMES ANDARY
TECHNICAL OFFICER
26 FEBRUARY 1988

# TABLE OF CONTENTS

# 1.0 EXECUTIVE SUMMARY

A multidisciplinary team of engineers and scientists from five universities has examined major aspects of safety for the Flight Telerobotic Servicer (FTS) program. The team has identified several requirements for safe operation of the FTS. They include an overall monitor (or watchdog) system, a single clear line of control at all times, special modes and sensors that apply when an astronaut is inside the FTS' work envelope, confirmed reporting of current status, and manual modes for testing and emergency situations.

## TERRESTRIAL EXPERIENCE WITH ROBOTS

Terrestrial industrial experience is applicable to FTS's development and use. A checklist of FTS safety issues has been developed, based on experience with terrestrial robots. It covers:

Environment
Programming
Hazard assessment
Training and certification
Mechanical considerations
Electrical considerations
Procedures

Key points of the checklist are:
Need for EVA control when an astronaut is nearby
  FTS status must be available continuously to the astronaut
  FTS must have astronaut sensing devices
Assurance that stored energy is released safely
Safety software in the control system

## HUMAN PERFORMANCE

New methods of modeling human performance can facilitate the use of FTS. Simulations will be important at all stages of FTS life.

Human response to FTS system failures deserves special consideration. Several power-up modes could allow recovery from failures. For example, a "weak and slow" robot mode could minimize the danger to an astronaut who must free a manipulator manually. Perhaps several programmable levels of robot "strength" and "speed" would be useful.

When a task involves three participants (two astronauts and the FTS), there must be a single point of control. It may shift with time as new subtasks are performed. However, team members should learn about changes and acknowledge their acceptance of them before the next phase or subtask begins.

A speech synthesizer in the FTS might be beneficial. The telerobot could then "announce" completion of subtasks and plans for the next operation. This would improve communications, a vital element in safety.

## SOFTWARE

Development and design of FTS software is a key challenge. The following are major considerations in software development and evolution.

A design philosophy for validation and verification (V&V) must be applied to every software module. Methods such as design analysis, technical review, and testing must be applied in all stages. For rule-based AI software, system requirements, design and development details, and test plans must be documented.

The anticipated FTS tasks must be analyzed to identify operating modes. Safety considerations can then be defined for each mode.

An overall system monitor (or *Watchdog*) should be part of the safety-related software. Although it may be costly, the Watchdog should cover all, or at least most, safety aspects. There must be a specification of any omitted items.

## NASREM ARCHITECTURE

The FTS's computer architecture is assumed to be derived from the National Bureau of Standards Standard Reference Model (**NASREM**) for telerobot control systems. NASREM allows for a planning mechanism that provides intrinsic system safety through its operation under hazardous conditions. The planning mechanism uses anomaly detectors and anomaly mappers that generate contingency plans after:

Identifying subtasks that are hazardous and hence unexecutable;
Using evaluations of these subtasks in future plans.
Validating the safety system by demonstrating how specific sets of anomaly detectors work in test cases.

## WORKSTATIONS

FTS workstations should have the following characteristics:

Require minimal training for special tasks
Provide standard interfaces with easy hookup
Use graphical languages and other modern user interface features
Provide automatic methods for viewing robot motions and reach.

Workstation development provides many opportunities for technology interchange. Equipment designed for the physically disabled and commercial user interfaces can be sources of new ideas. Notational systems derived from choreography and music might provide effective ways to direct and monitor moving robots. Systems-Assurance analysis developed for KSC launch activities and nuclear power plants may be useful in developing safety procedures.

## DESIGNING SAFE SPACE STATION SYSTEMS

Safety issues must be key factors in FTS design, development, and evolution. The FTS and the Space Station system should be designed to work together with maximum safety for the astronauts, the robot, and the Station's operating and scientific subsystems. The earlier in the design process this is recognized, the better. If such design and development work is successful, the FTS—Space Station combination will be more robust, and more intrinsically safe, than the Station by itself. There are several reasons for this. The Space Station is much bigger than the FTS and less testable. A properly designed and tested FTS can improve safety by performing part of the regular inspection and maintenance of the more fragile Space Station. The FTS can also improve Space Station safety by reducing the need for EVA and by allowing more appropriate allocation of tasks for astronauts.

## PARTICIPANT TEAMS

TERRESTRIAL INDUSTRIAL EXPERIENCE
Dr. L. Ken Lauderbaugh*
518/276-6983
Ms. Davetta Montgomery
Mechanical Engineering Dept.,
Troy, New York 12180-5390

RENSSELAER POLYTECHNIC INSTITUTE

HUMAN PERFORMANCE MODELING
Dr. George Kondraske*
817/273-2335
Ms. Katy Hoard
Human Performance Institute,
Arlington, TX 76019

UNIVERSITY of TEXAS at ARLINGTON

NASREM ARCHITECTURE
Dr. Michael W. Walker*
313/764-6894
Dong-Min Kim
Robot Systems Division
Dept. of Electrical Engineering
and Computer Science,
Ann Arbor, MI 48109

UNIVERSITY OF MICHIGAN

SOFTWARE
Dr. Kai-Hsiung Chang*
205/826-4330
Dr. James Cross
Mr. Steve Dannelly
Dept. Computer Science & Engineering,
Auburn, AL 36849

AUBURN UNIVERSITY

PROGRAM DIRECTOR
Dr. David R. Criswell, Consortium for Space/
Terrestrial Automation and Robotics
619/534-2047
University of California, San Diego
M.S. A-016
La Jolla, CA 92093-0216

California Space Institute kindly hosts C-STAR. We are fortunate to have had the professional expertise of two of CalSpace's staff members:
Dr. Mahmoud Tarokh and
Mr. Philippe Collard

* Principal investigator.

# 2.0 OVERVIEW

Congress specifically directed that a robot, designated the Flight Telerobotic Servicer (FTS), be developed and deployed with the first elements of the Space Station for use in construction and maintenance. It would also service external experiments and satellites.

Congress wanted to support the development of new tools for space work and to advance the technological position of United States industry in advanced robotics.[1] NASA reports every six months to Congress on its progress in nurturing advanced automation and robotics within the Space Station program and on the development and eventual use of the FTS.[2]

Responsibility for developing the FTS was assigned to Goddard Space Flight Center (GSFC) in 1986, approximately one year after the start of detailed planning for the Space Station. There is no doubt that robots will be needed on the Station because of severe manpower limitations. Only six crew members are scheduled to occupy the station at first. The station will be the largest and most complex object ever placed in space. The crew's attentions should be on projects the Station will support rather than on upkeep. The FTS is to be a primary on orbit aid for automated maintenance. It should also provide significant support in the Station's construction, or first element launch (FEL), phase.

Maintenance is an essential part of a long-term program like the Space Station. Astronauts did extensive EVA repairs to the U.S. Skylab and Soviet Mir station that enabled their missions to continue. However, lack of a robotic tug to attach to and boost Skylab resulted in the loss of a usable facility. The Soviets have used such tugs to resupply the Mir station.

The United States has used a limited robotic arm, the remote manipulator system (RMS), onboard the orbiters.[3] The RMS is used to deploy and retrieve payloads from the orbiter bay, capture satellites, provide a work platform for astronauts, and inspect the sides of the vehicle. The RMS is a relatively light structure with limited strength. It is too fragile to be used on Earth and is only operational in the zero-gravity of orbit. RMS is representative of a more advanced arm to be used by the mobile servicing center (MSC) planned for Space Station. The RMS has proved extremely useful within the Space Transportation System (STS), even under conditions beyond the original design constraints. However, on orbit testing has led to the imposition of operational limitations. For example, the vernier rockets of the orbiter are not fired when the RMS is extended and attached to large payloads. The FTS can be a far more rugged device that the RMS or the equivalent arm of the proposed MSC for Space Station and will certainly be more compact. Thus, FTS can be tested aggressively on the ground and its use planned with far greater confidence than could that of the RMS or MSC.

## 2.1 NEED FOR STUDY AND FOCUS

Studies of industrial safety far predate NASA. However, NASA is unique in making safety a paramount concern in virtually all aspects of its operations. NASA draws on the safety experiences of industry and also returns technologies and safety techniques to the national economy. For example, tools developed to analyze rocket launch reliability at the Kennedy Space Center[4] have industrial applications such as safety systems for nuclear power plants.

The FTS will present NASA with many safety concerns. It should provide new ways to enhance the safety of space operations. For example, the FTS should reduce the need for EVA, increase EVA productivity, inspect completed work and provide objective recordings to others, and later operate with orbital transfer vehicles at great distances from the Space Station. FTS can serve as a model for new tools specific to space, new options to aggressively maintain safety of the station on orbit, and new ways to test concepts in assembly or module changeout. Such uses of FTS could shorten the design cycle. In addition, safety lessons learned while developing and using FTS could find applications in the nation at large.

The FTS Program Office at GSFC decided to support a broad study by researchers from four universities to identify major safety issues. Each university provided experience from a different research area. The study was organized and administered by the Consortium for Space/Terrestrial Automation and Robotics (C-STAR), a division of the Universities Space Research Association (USRA). For the period (August 1987 - January 1988) of this study, C-STAR was headquartered at the California Space Institute of the University of California at San Diego. The four principal investigators, their universities, and their areas of investigation are listed in the Executive Summary (Section 1.0).

Conceptual design of the FTS and its applications begin in late 1986. At the start of the Human-Robot Safety (HRS) study, only a strawman design of the FTS was available.[5] Several example FEL tasks for FTS to perform during assembly had been identified. They included connecting thermal pipes, installing electrical and other lines in utility trays, inspection, and assembly of structural components. Clearly, the team could consider a very wide range of operations, types of robots, and environments. However, in view of the preliminary nature of both the study and the status of the FTS and Space Station architectures, NASA and the project team decided to focus on a particular task. Two iterations were required.

The first meeting of the HRS Project Team occurred on August 25 (evening) and August 26, 1987, at the Goddard Space Flight Center in Greenbelt, Maryland. The following scenario was chosen as the reference for safety issues: Suppose the telerobot fails to release a high pressure pipe joint, and an astronaut must go EVA to determine the problem. This "worst case" approach, although dramatic, was found useful in identifying key safety issues. NASA provided the team members with the following materials:

- Videotape of truss assembly simulation
- Artwork showing FTS "at work"
- Briefing slides of the presentations made during the meeting
- NASA handbook on EVA.

The second meeting of the HRS team occurred at the Jet Propulsion Laboratory onNovember 21-22, 1987. At that meeting, the team decided to focus on the connection of electrical utilities and utility trays. This was driven primarily by the desire to consider a more detailed example of a task that would take advantage of the NASREM computer architecture. A description of connecting utilities was available in the documentation of the strawman FTS.

## 2.2 BROADER CONSIDERATIONS

Sections 3 through 6 present the results of the Auburn University, Rensselaer Polytechnic Institute, University of Michigan, and University of Texas-Arlington teams. Because Cal Space has been active for several years in planning automation and robotics for the Space Station, it considered the broader implications of the FTS for Station design, implementation, operation, and evolution. Section 7 discusses the general topic of designing for safety.

FTS is the first serious effort to develop tools specifically to leverage the precious work hours of IVA and EVA astronauts. Operations planners could reserve EVA for key tasks such as final certifications at the system level. They could develop contingency plans that focus on the best use of EVA astronauts in dealing with unanticipated problems that require the full capabilities of humans.

FTS will be left on orbit from the first FEL mission. Continuing review of STS schedules will likely reveal situations in which it will be vital to have a mobile FTS available to work under ground control. FTS can be used to create new options for assembly that are not constrained by the limited EVA time allowed during the FEL period.

The advantages of having more than one FTS should be explored aggressively. Multiple FTSs might eventually be teamed with astronauts to allow wider dispersal, while still maintaining safety equivalent to the EVA buddy system. The use of FTS subsystems in an "active" inventory should be considered. For example, FTS gripper or control units might be used for IVA laboratory operations and yet still be available for changeout with a full unit.

Mobility is a critical issue in FTS development and application. It would greatly extend the FTS's range of tasks. Mobility might be provided by a detachable plug-in unit. However, this possibility must be anticipated.

Because the FTS is a computer/data intensive system, it can in principle be self-documenting. It can supply data on both normal and unusual operations. Such data can be used to help reprogram other FTS or spare subsystems without the long training periods required by astronauts. During design and testing of Space Station components, FTS subsystems can be used for documentation like a standard astronaut with perfect memory.

## 2.3 REFERENCES

1. "Automation and Robotics for the National Space Program," 127 pp., by the Automation and Robotics Panel (ARP), California Space Institute of the University of California, headquarters University of California at San Diego, NASA Grant NAGW629, 1985.
2. "Advancing Automation and Robotics Technology for the Space Station and for the U.S. Economy: Progress Report #5," Advanced Technology Advisory Committee (ATAC), 1987, 46 pp., NASA Technical Memorandum 100777, September (see also TM - 89811 (May 87), - 89190 (September 1986), - 88785 (March 1986), - 87772 (September 1985), and - 87566 (April 1985).
3. Peters, W.L. "Space Shuttle Remote Manipulator System—Development and Certification," Johnson Space Center, code EF2, p.27, 2 December 1987.
4. Page, D. W. "Application of NASA Kennedy Space Center Systems Assurance Analysis Methodology to Nuclear Power Plant Systems Designs, Nuclear Engineering and Design," vol. 89, pp. 391-403. (see also NASA Tech. Brief KSC-11306), 1985).
5. Flight Telerobotic Servicer (FTS) Strawman Concept Engineering Report, NASA Goddard Space Flight Center (GSFC), SS-GSFC-0031, March 15, 1987.

# 3.0 ROBOT SAFETY: INDUSTRIAL EXPERIENCE

Dr. L. Ken Lauderbaugh
Ms. Davetta Montgomery

Mechanical Engineering Dept.
Rensselaer Polytechnic Institute

## 3.1 INTRODUCTION

### 3.1.1 Background and Approach

This chapter is the product of a study of many journal articles and reports that discuss the issues of terrestrial robot safety, especially the experiences gained from the studies of robot accidents and safeguarding procedures. This study culminated in recommendations for the safe design of the Flight Telerobotic Servicer (FTS), presented in the form of a safety checklist.

### 3.1.2 Organization of Chapter

The chapter has three main sections. The first section discusses terrestrial robots, beginning with a compilation of information available on robot fatalities, accidents, and near accidents. The study of terrestrial robot accidents points up the areas where safeguards are necessary. This section also contains information on domestic and international robot safety standards. It concludes with intrinsic safety design guidelines for terrestrial robots and robot systems.

The second section discusses FTS robot safety. It begins with safety design guidelines specific to the FTS application and concludes with an FTS hazard assessment checklist.

The final section discusses some developmental work that remains to be done.

## 3.2 TERRESTRIAL ROBOTS

### 3.2.1 Fatalities, Near Accidents, and Accidents

One way of recognizing the requirements for robot safeguards is by studying robot accidents. Accident reports are difficult to locate, and the authors were unable to identify any United States agencies that collect reports of accidents involving robots. As an example, while the National Safety Council was able to furnish a bibliography of reports and articles which deal with robot safety and robot accidents, it does not collect data or generate statistics on fatalities, near accidents, or accidents.

A few sources from outside the United States present such results, summarized in the following two sections.

#### 3.2.1.1 Fatalities

Despite their high operating speeds and often unpredictable movement, the total number of fatalities associated with the operation of robots is much less than with other industrial machines. To date, five reported and documented fatalities internationally have been associated with the operation of industrial robots.[1] The most recent fatality occurred in the United States and the previous four occurred in Japan. The higher incidence of fatalities in Japan may be attributed to two things. The Japanese definition of robot[2] includes many more classes of industrial equipment than the definition in the United States. Japan also has longer experience with industrial robots.

The five fatalities are:

1. Japan, July 1981. A repairman climbed a safety fence to work in a robot's work space while the robot was operating. The robot pushed him from the rear into a grinding machine and he died.
2. Japan. A worker climbed onto a moving conveyor while a robot was idle, but still operating. The robot moved and squeezed him to death.
3. Japan. A worker reactivated a robot after servicing a machine near it. The robot moved, pinning and crushing the worker to death against the machine.
4. Japan. One worker started a robot while another worker was in the robot's work space. The robot pushed the second worker into a positioning fixture and killed him.
5. US, July 1984. A worker was pinned by a robot against a pole and crushed. He died 5 days later. A legal suit was filed and his family was awarded 10 million dollars.

These fatal accidents have four things in common.

1. In almost all cases, the worker entered the robot's work zone to correct a minor problem in interfacing equipment like conveyors or metal working machines, but not in the robot itself.
2. While in each case the worker was experienced, he did not follow safety procedures, was complacent, took unnecessary risks, or was in error.
3. The robot struck the worker from behind without warning.
4. The worker was pinned by the robot against another machine or a structure in the work space, and the worker was killed by the other machine or by crushing.

From these commonalities, needs for safeguarding procedures become apparent. For example, it is clear from point four that a robot's work space must be designed to permit clearance for operators to move safely between the robot and other equipment. Much of the remainder of this report is devoted to the discussion of this very important issue of safeguarding against accidents.

### 3.2.1.2 Near Accidents and Accidents

As with the discussion of fatalities, common points can be drawn from the studies of near accidents and accidents, and needs for safeguards can be identified.

**A Swedish Study.** A robot accident is defined as an occupational injury in which a robot is involved. The report of a study conducted in Sweden from 1979 through 1983[3] summarized 36 reported robot accidents. In almost all cases the robot was a manually controlled manipulator, which was performing pick and place operations.

One finding from the Swedish study was that most contact occurred during adjustment in the course of operation (14 cases) or during repair, programming, or other operations (13 cases). This is in agreement with other studies that showed that of the four principal modes of operation: installation, teaching, normal, and maintenance, teaching and maintenance are the most hazardous modes, during which the largest chance of injury to workers exists. This is because during teaching and maintenance it is often necessary to have a worker within the operational envelope of a active robot.

If an active robot makes an unexpected movement, a human worker in its work cell is in danger of being struck. The possible causes of unexpected movement include, but are not limited to, software error, control problems, component failure, electrical noise, oil pressure valve trouble, encoder related problems, and electronic malfunction. In addition, human errors, such as accidentally or prematurely returning a robot to power-on position when a worker is in its work cell, cause many injuries.

The Swedish study reported injuries to the following parts of the body: finger (12 occurrences), hand (7), arm (2), back (4), head (6), neck (1), leg (2), rib (1), tooth (1). Even with the number of head injuries, most workers required only short periods of sick leave. There were no fatalities.

**A Japanese Study.** A Japanese study of robot accidents found that over thirty-eight percent of reported accident situations were the result of erroneous actions of robot operators.[4] When the design of a robot is not intrinsically safe, itssafe operation depends heavily upon the skills of the person working with it, and the risks associated with operation are increased. This explains the importance of training and continually retraining people who work with robots, in order to improve their skills and reduce the occurrence of accidents.

**Common Points.** Some common points appear in these and other reports[5] of human injuries from robot accidents.

1. The majority of injured workers are operators or maintenance personnel; however, the curious and risk taking outsider may make unauthorized entry into the robot's work space and be in danger.
2. Robot gripper to human hand contact is most typical.
3. Workers are sometimes trapped or pinned by the robot against other equipment or the work space enclosure.
4. A robot manipulator may release an object during normal or aberrant operation, or during a stop, and that object may contact and injure a worker.

It is important to recognize that a robot may appear "dead" to a worker, when in fact it is powered and in a software dictated hold period, waiting for its next move command. A worker could interpret this inactive status as powered down and approach the robot, placing himself or herself in danger. To safeguard against this hazard, rotating lights should be positioned on the top of robots to indicate a power-on condition. This indicator is usually fail-safe, since failure of both the bulb and of the rotating mechanism are required for indicator failure.

### 3.2.2 Terrestrial Robot Safety Standards

Because of a robot's operational characteristics and its unique nature of association with operators and maintenance personnel, safeguarding standards for traditional industrial machines and equipment are not applicable to robots. Discussions of the necessity for and the development of safety standards for industrial robots and robot systems were contained in many reports and articles.[4,6-11] Domestic and international standards and comments about them, where available, follow.[2]

**USA**: ANSI/RIA 15.06 "American National Safety Standard for Industrial Robots and Industrial Robot Systems" Robotic Industries Association, 1986.

Objective of the standard is to enhance the safety of personnel who work with industrial robot systems by establishing guidelines for the construction, installation, care and use of industrial robots. Compliance is voluntary. The standard specifically excludes space robots. The standard may be ordered from RIA or ANSI.

**UK**: Machine Tools Trade Association (MTTA). "Safeguarding Industrial Robots, Part 1: Basic Principles" 1982.

MTTA, with Health and Safety Executive (HSA) assistance, developed a industry code of practice covering hazard identification, risk assessment and safeguarding of industrial robots, with emphasis on programming and maintenance modes.

**USSR**: GOST-SSBT. "Industrial Robots, Robotised Installations and Robotised Shops" 1982.

**Japan**: JIS B 8433. "General Code of Safety for Industrial Robots" 1983.

**West Germany**: VDI Guideline 2853. "Safety Requirements Relating to the Construction, Equipment and Operation of Industrial Robots and Associated Devices" 1984.

**East Germany**: TGL 30267/01. "Industrial Robots for Machine Tools; Terms; Requirements, Safety Measures" 1982.

**France**: AFNOR Standard, in preparation.

Letters requesting copies of the safety standards were sent to the robotic safety agencies of Sweden, Canada, Japan and Great Britain. Japan and Great Britain replied as of the date of this writing; the Japanese sent a purchase order for their standard written in Japanese, not English, and Great Britain sent literature, but did not include standards information.

The discussion now turns to safeguarding through intrinsic design and operation guidelines.

## 3.2.3 Intrinsic Safety Design and Operation Guidelines

The most certain way to ensure safe operation of a robot system is to design the system for intrinsic safety. The Merriam-Webster Dictionary defines "intrinsic" as "belonging to the essential nature or constitution of a thing." An intrinsically safe system therefore is one that operates safely, independent of external systems. Designing for intrinsic safety is important for two reasons: The safe operation of a robot that is not intrinsically safe additionally taxes the robot operator's skills. And operator errors cause a significant percentage of industrial accidents,

A number of sources that address the design for intrinsic robot safety were identified.[13-18] Two other sources[19-20] provided general hazard assessment checklists comprised of a lists of questions that alert robot system designers to specific safety issues, and thus help the designers improve the intrinsic safety of their systems. These checklists served as a frame for the FTS hazard assessment checklist presented in section 3.3.2.

The following sections discuss safety issues characteristic of specific areas of robot system design. While the issues are discussed in the context of terrestrial robot safety, many of the intrinsic design and safeguarding procedures are equally applicable to the space environment. Developing upon these terrestrial safety issues resulted in the checklist presented in section 3.3.2.

### 3.2.3.1 Robot Programming

The act of programming a robot to perform a series of actions is referred to as teaching. Below are many common concerns for safe operation of a robot during teaching.

1. When a robot is in the teach mode, whether it is controlled through a mobile teach pendent or the main console, it is recommended that the robot operate at a slow velocity. Although it is difficult to generalize from one robotic system to the next, a maximum velocity of 250 mm/sec has been suggested by many sources, including the American National Standard. (In space this maximum velocity will need to be lower.)
2. The teacher should have complete control of the robot, especially when within the robot's working envelope.
3. Control of the robot by two or more teachers should be avoided.
4. Restart of the robot should be possible only from outside the robot's work cell and only after all systems have returned to normal operation.
5. The teach pendent should have a three position deadman switch which initiates an emergency stop if the handle is either released or squeezed too tightly, as it may be in an emergency or panic situation.
   a. This switch should be deadwired to the stop circuit, and not pass through software links, which when down, could fail to prevent an emergency stop.
   b. There should be separate drive and encoder disconnects, so that when the robot is powered down in an emergency stop situation, position data are not lost.

### 3.2.3.2 Protecting Against Human-Robot Contact

Experience has shown that it is necessary to have layers of protection between the robot and humans who share the robot's work space. The outermost layer is a peripheral barrier. If the peripheral barrier is penetrated, presence sensing capabilities are required to alert the robot's safety system to an invasion. They must also initiate an emergency stop or activate a collision avoidance routine.

**Barriers.** The outer layers of protection for a worker from a terrestrial robot are peripheral barriers, like fences, ropes, and chains, to prevent him or her from entering the operating robot's cell. In addition, the work cell may be delineated with lines painted on the floor or signs hung in the area.

The most effective barrier for preventing unauthorized access is an electrically charged interlock fence (obviously impossible in space). Through control circuitry, power to the robot is interrupted when an interlock fence is opened. Power cannot be restored until the gates are secured and an operator activates a restart button positioned outside the peripheral barrier.

**Presence Detecting Devices.** As mentioned earlier, many accidents occur when curious or complacent workers penetrate a peripheral barrier and enter an active robot's work cell. In these instances, it is desirable to equip the robot with an intelligent means of detecting workers and preventing contact with them.

The inner layer of safeguarding against human-robot contact is the application of presence detecting devices that are linked to the robot's safety system. The simplest kind is a pressurized floor mat that causes an emergency stop of robot activity when stepped upon. But often it is necessary to employ more sophisticated tactile, proximity and range, and machine vision devices for presence detecting.[21-25] Many of these sensors detect not only a human's presence, but also an object entering the working envelope or objects within the envelope changing positions. Some presence detecting devices are:

- light curtains/photoelectric sensors
  (photoreceptor and infrared directional light source)
- motion sensors:
  - ultrasonic (echo-ranging)
  - microwave
  - infrared
  - capacitance
- magnetic field detectors
- vibration sensors
- acoustic sensors
- supersonic
- laser
- visual
- hall effect
- inductive
- electrostatic
- sonar

Each of these sensing devices has specific capabilities, ranges of operation, and reliability. By incorporating more than one type of sensor into a sensory system, that is, by utilizing multiple sensor integration (MSI), the overall safety level of the robotic system can improve. Sensory information from more than one source is combined and compared to give more accurate information in real time, reducing the impact of a single sensor's failure.

Many features must be considered when selecting sensors and sensory systems to operate in real time. Ideally, the sensors should have the following properties:

- high accuracy
- high precision
- operating range broad enough to encompass all possible hazards, but not so broad that they take in extraneous information that would delay processing
- quick speed
- fast response
- compatibility with other components
- compatibility with the environment in which they operate
- easy to calibrate and hard to work out of calibration
- high reliability with large mean times between component failures
- straightforward operation, with minimum room for misunderstanding or improper operation
- simple and easily understandable (for both system operators and interfacing equipment) output characteristics

**Collision Avoidance.** Once a worker's presence has been detected by the sensors in the inner layer of protection just discussed, the next step is collision avoidance, the simplest form of which is emergency shut down of the robot. A safety monitoring and control system[26] is being developed, because it has been recognized that emergency shut down may not always be practical or desirable; sometimes a human must share an active robot's work cell, for example, during teaching and maintenance.

One sophisticated collision avoidance systems is a stand alone safety system developed at Rensselaer Polytechnic Institute.[27-29] This system uses capacitance and acoustic elements and employs special mapping algorithms and dedicated processors to map and memorize features within the operating range of the robot. When defined parameters are violated during robot operation, corrective actions are taken.

Also under development is a "Watchdog Safety Computer" system,[30] an auxiliary safety computer that monitors status and sensory inputs from the robot, the controller, and other sources. When it receives information out of specification, the safety computer powers down the robot and notifies the system operator.

#### 3.2.3.3 Kinetic Energy Control

The issue of controlling a robot's kinetic energy is often discussed in the literature. It is important to incorporate methods of dissipating stored energy, especially during emergency power reduction, into the design of a robot's components. Specific approaches to controlling and dissipating kinetic energy are discussed in section 3.3.1.6.

## 3.3 FTS ROBOT

The first issue to be presented in turning to the operation of the FTS robot is recommended safety design guidelines, based on conclusions drawn from operating experience with terrestrial robots. Section 3.3.2 presents a hazard assessment checklist for FTS systems designers to use in determining whether safety has been designed into each system.

### 3.3.1 Intrinsic Safety Design and Operation Guidelines

This section presents a series of design and operation recommendations that have great impact on the FTS system's intrinsic safety. Some of these issues are specific to the space application of robots and robotic systems, while others are terrestrial issues that have been tailored to space use.

#### 3.3.1.1 Environmental Concerns

Terrestrial robots typically operate in a very well defined and predictable environment, where the environmental conditions usually do not vary widely. Conversely, the FTS robot will operate in the dynamic space environment, where the world model is continually changing. Many of the sensors available today may not be able to meet the demands of operation in space. This presents us with the unique challenge of designing sensors and computational techniques capable of updating the dynamic world model in real time.

The fact that the FTS will operate in space presents many additional design challenges. When formulating all component and system designs, the hazards associated with exposure to and operation in the space environment must be considered. For example, designs should safeguard against damage from:

- electromagnetic radiation (EMR)
- earth generated radio frequency noise
- penetrating charged particles (ionizing radiation)
- meteoroids and space debris
- neutral atmosphere density
- induced environment and effects
- magnetic fields
- earth's gravitational effects
- plasma environments

and all other environmental conditions outlined in NASA Document JSC 30425 and references therein.

### 3.3.1.2 Operational Modes

NASA document SS-GSFC-0031 states that there are four modes of operation for the the FTS: teleoperation, both with EVA and without EVA; autonomous; combined teleoperation and autonomous; and transitional between teleoperation and autonomous. In addition, aberrant operation must be expected. Safe and appropriate responses to system and component failures must be preplanned and programmed into the operating software, to prevent accidents. At the very least, the FTS should be safely powered down.

**Teleoperation.** The fact that the FTS will be teleoperated poses unique safety problems. First, the state of the art in teleoperation will need to be advanced to satisfy the requirements of the space application. Further developments of the state of the art in safety systems for teleoperated robots will also be required.

One of the strongest recommendations involves teleoperation of the FTS while an EVA astronaut is within its working envelope. In this case, the EVA astronaut should have complete control of the FTS. Evaluation of the issues surrounding accidents and fatalities resulting from robot-human contact supports this recommendation. The greatest danger of accident or death occurs during teaching and maintenance, times when the worker is closest to the robot. For the worker to have anything less than complete control of the robot is extremely dangerous.

While it may be advisable that two astronauts work together when on EVA near the FTS, dual control of the FTS is very dangerous and should not be possible. One astronaut should have complete operational and shut down control, while the other astronaut has only emergency stop control. (All EVA crew members should have FTS emergency stop control designed into their space suits.) Recall the fourth fatal accident cited: One worker returned a robot's power before a second worker was out of the robot's work envelope, and that second worker was killed.

Return to autonomous mode of operation after teleoperation should be prevented until it is verified that all EVA astronauts are outside the robot's work envelope. It must be determined whether initiation of autonomous operation should be possible from a mobile teach pendent or only from the main console.

### 3.3.1.3 Preventing Astronaut-Robot Contact

NASA documents point out that while some of the astronaut crew will be FTS certified and some will not, all astronauts who enter the FTS work space during EVA must be protected. As previously mentioned, one way of protecting the authorized EVA astronaut is to ensure that he or she has complete FTS control. But what about preventing unauthorized entry by an EVA astronaut into the FTS robot's work space? One terrestrial way of safeguarding against this is to put up protective barriers and lay down pressure sensitive mats. Needless to say, there must be a different approach to preventing astronaut-robot contact in space.

Safeguards must be available to prevent accidental contact or collision between the robot and an EVA astronaut. The problem can be approached from two sides: How can we make an astronaut aware of the robot's position and activity? How can we make the robot aware of the astronaut's position and activity? An industry-proven way of alerting a worker to the status of a robot has been a visual display, such as a rotating light atop an activated robot. This alone is not enough of a safeguard, because an astronaut could still unknowingly drift backwards into the robot, and be struck by the robot. In consequence, focus must turn to the second approach to solve the problem of preventing astronaut-robot contact.

Astronaut presence-detecting proximity sensors like those discussed in section 3.2.3.2 could be incorporated into the FTS system. Appropriate FTS reaction, for example, power down, speed reduction, or avoidance, could be programmed into the FTS operating software or safety system software. In space, an EVA astronaut has the advantage of always wearing a space suit that can include sensors and transmitters as part of the presence sensing system. Thus, if an astronaut were to drift unknowingly into the FTS robot's work space, the robot would be able to recognize the astronaut and react to avoid contact. To return to the first approach, information from the presence-detecting devices could be relayed by way of an audio warning signal or a "heads up display" in the astronaut's space suit to inform him or her of the robot's status and distance. The astronaut would then be able to react to avoid the robot.

It is human nature for people to become overconfident or complacent, sometimes shortcutting safeguards. To protect against this temptation, guards against improper astronaut use of the FTS must be designed into the FTS robot and operating systems.

#### 3.3.1.4 Training

The strongest means of safeguarding against astronaut-robot contact is training and retraining the crew members in FTS operation and safety procedures to reduce the operator's contributions to accidents. Initial training must be rigorous and thorough and should follow training documents which are easily understood and readily referenced. Periodic retraining is essential to refresh the astronauts' memories and, in addition, to prevent the astronauts from either taking risks or becoming complacent.

#### 3.3.1.5 Reliability

The useable life of the FTS is estimated to be at least thirty years, so each component must be designed with concern for component and system reliability. Following a formal preventative maintenance and replacement schedule is essential to the reduction of equipment failures and the safe operation of the system.

#### 3.3.1.6 Energy Release

Special attention should be paid to the safe release of energy stored within the FTS. Industrial accidents involving robots have been classified as energy-conversion accidents, where the stored energy of the robotic system is mischanneled into a form which injures people.[2] High levels of kinetic energy are especially dangerous in the event of collisions, and control becomes more complex and less reliable as the level of kinetic energy increases.

Kinetic energy levels can be reduced in a number of ways. Although the obvious approach is to limit speed, it is equally important to optimize the design of the robot's arms to minimize arm inertia. Arm material, mass distribution, and shape must all be considered.

Kinetic energy absorption through the use of mechanical stops, shock absorbers, damping and dynamic or frictional braking can also be incorporated into the design of the FTS. Or the kinetic energy could be converted to elastic energy of spring type components.

Electrical, thermal, radioactive, and high pressure energy sources should also be identified and safe release of those energies incorporated into the FTS design.

### 3.3.2 FTS Hazard Assessment Checklist

To safeguard a robotic system against possible component failures, a hazard identification check should be made of each component's design. The FTS hazard assessment checklist presented here grew out of terrestrial experiences and checklists like those discussed in section 3.2.3, modified for the space environment. It can be used to alert FTS designers of safety issues that should be considered, thereby improving the intrinsic safety of each component and the entire system.

When using the checklist, it is important for the designer to consider the source of the hazard and design a safe means for its elimination.

#### 3.3.2.1 Environment

• Do all system designs (control system, actuators, power supplies) safeguard against damage from the most severe combinations of natural environments, including:

- electromagnetic radiation (EMR)
- earth generated radio frequency noise
- penetrating charged particles (ionizing radiation)
- meteoroids and space debris
- neutral atmosphere density
- induced environment and effects
- magnetic fields
- earth's gravitational effects
- plasma environments

and all other environmental conditions outlined in NASA Document JSC 30425 and references therein?

### 3.3.2.2 Mechanical Systems

- Is the FTS securely locked to the space station structure so as to prevent accidental release or movement when operating in the fixed-base detached mode or special case umbilical mode?
- When operating off the end of the transporter arm, is the FTS securely locked in order to prevent accidental release or movement?
- When positioning the FTS at the work site, is adequate clearance from the space station structure and other equipment assured to avoid contact and pinch points? Is there enough clearance for an EVA astronaut to prevent pinning?
- If the FTS is operating while connected to the transporter arm, is adequate clearance from the space station structure and other equipment assured to avoid contact and pinch points? Is there enough clearance for an EVA astronaut to prevent pinning?
- Do grippers retain the tools or work piece during emergency stop or power loss to avoid accidental release?
- Have the end effectors been designed fail-safe by using more than one gripping mechanism?
- If gripper release during power loss can not be assured, would tethering be possible?
- Have the proper interfaces with remote material handling been included?
- Are gears and pinch points covered with guards?
- Have all sharp edges and corners been eliminated or covered, especially on the grippers?
- Is the FTS's exterior free of protrusions which may cause snagging or tearing of an astronaut's space suit?
- Are drive mechanisms covered?
- Is the FTS's exterior free of hoses or cables in which an astronaut or equipment could become entangled?
- Are all hoses secured or internal to prevent swalling in case of a ruptured line or broken connection?
- Have means of controlling vibration disturbances been implemented?
- Does the robot react appropriately (power down or slow down and avoid collision) when an unauthorized EVA astronaut enters its work envelope?
- Is it possible for the FTS to avoid a collision with an EVA astronaut through path planning?
- What are safe velocities for the grippers during the different operational modes: teleoperation (with EVA, without EVA), autonomous, teleoperation and autonomous, transitional?
- Are the robot arms able to withstand the maximum possible working loads and torques?
- Are hardware stops and brakes strong enough to stop the robot arms when they are moving at their top speeds and carrying their maximum loads?
- Is the robot adequately protected when in storage?
- Are electrical cables protected from excessive wear during arm movement to prevent fraying and possible short-circuiting or shocking?
- All all cable connections secure?
- Does the system contain stored energy that could cause damage to the FTS, other equipment or an EVA astronaut if inadvertently released? Have all of the following energies been considered?
  - kinetic energy associated with robot motion
  - high pressures in fluid lines
  - electrical energy that could result in electric shock
  - chemical or biological energy from sources in area
  - thermal energy from radiation
  - radioactivity

### 3.3.2.3 Electrical Systems

- Have sensors been included to monitor the power supply to the FTS robot?
- What is the effect of loss of power or interruption of power to the system?
- Are the power supplies adequately filtered to prevent damage in the event of power surges?
- If power down is desired whenever an EVA astronaut enters the FTS's work envelope, have all presence sensing detectors been wired in series with emergency stop circuits?
- Can the "hold the last state" controls be overridden in the event that a gripper has trapped an EVA astronaut?
- Have adequate controls been installed to prevent a collision of movable equipment in the event of a software failure?
- Are FTS robot activity status and position information available to all EVA astronauts? Is an activity status a visual signal like a revolving light displayed on the FTS robot? Do the astronauts have a "heads up" display of the robot activity status?

- Is the power control a deadman switch which must be depressed to activate and which when released causes motion to stop? Is it a three position deadman's switch which also causes motion to stop if it is squeezed too tight, as it may be in a crisis situation?
- Are emergency stop switches readily available to all EVA astronauts? Is the switch incorporated into the design of the space suit?
- Are emergency stops hardwired to interrupt the power supply to the robot drives, disengage clutches and activate brakes?
- Are there fail safe features to guard against short circuits and other failures?
- Do the electronics have guards against contact bounce?
- Is the speed of response of the safety system sufficiently fast for worst case conditions?

#### 3.3.2.4 Operating System

- Is the main memory held in nonvolatile form?
- In what form is the program held?
- Is memory protected during planned or unexpected power loss?
- Is more than one program held in memory at one time? If so, can security between programs be ensured to prevent overwriting existing programs with data or prevent execution of jumps between blocks of memory?
- Is operation prevented if robot is out of calibration?
- How is program editing done? During reprogramming, can existing data be lost or altered?
- Is software operation clearly and efficiently documented and are the documents readily available to users?
- Is software user-friendly and easily operated?
- Does programming involve the use of a mobile teach pendent as an alternative to the main console? If so, is the teach pendent layout ergonomically designed? Are the controls clearly marked and well spaced to avoid inadvertent operation? Are the same points considered for an EVA teach pendent?
- Does the user of a teach pendent automatically remove control from the main console?
- Does the operating system software verify that all EVA astronauts have moved outside of the robot's work space?
- Has it been determined whether a complete cycle may safely be initiated by a mobile teach pendent, or must a complete cycle be initiated by the main console?
- Are there separate encoder and drive disconnects to preserve position memory in the event of drive disconnect (emergency stop)?
- When the speed of movement is varied, is it through primary power source reduction as opposed to control circuitry? (This will ensure a faster response unaffected by software or control failures.)
- Are specific safety interlocks contained in the software? If so, is their purpose to improve the safety of the system?
- Is program checking used during system testing and operation?
- Are a minimum of two manual actions required prior to restart after an emergency shutdown?
- Has a system been implemented to ensure that all safety violations have been removed prior to a system start?
- What diagnostic facilities are available?
- What is the effect of data loss during program loading?
- Can the robot be moved through an undefined pathway?
- Are safety backup systems operating?

#### 3.3.2.5 Sensory Systems

- Can the FTS sense an EVA astronaut in its work envelope?
- Can the FTS sense system or component malfunctions and notify the operational or control system as required?
- Can the FTS sense process conditions?

#### 3.3.2.6 Control System

*Note*: The following require the logic system to be active and the robot to be calibrated correctly.

- Has an assessment been made of the consequences of failure of the robot control elements?
- For each servo control drive, are the limits of arm speed and travel limits identified?
- Have appropriate responses to the following interrupts been programmed?
  - excessive following error on each servo control drive
  - abnormal velocity on each servo control drive
  - hardware travel limits
  - abnormal temperature, voltage, current sensors
  - communication data flow abnormalities
  - shutdown signals from outside interfaces
- Are operations inhibited pending the completion of other operations?
- Are there checks on the condition and function of control components for self diagnosis and prediction of performance deterioration?
- Can a controlled shutdown process be initiated under normal or emergency conditions?

#### 3.3.2.7 Astronaut Training and Certification

- Is astronaut training of FTS operation thorough?
- Are crew members thoroughly trained in software operation?
- Is periodic retraining performed?
- Are training documents available and easily understandable?

#### 3.3.2.8 General Concerns

- Has the design been researched to ensure that all codes and regulations have been complied with?
- Have safe design practices been followed in all of the FTS systems, including the mechanical, electrical, electronic, sensory, control and safety systems?
- Has a list of potential hazards been formulated? Are possible malfunctions included?
- Has each system and subsystem been tested in normal and aberrant operation?
- Are the modular components and subsystems designed so that they are compatible with existing interfaces? Are their designs flexible enough to be compatible with future modules?

## 3.4 FUTURE WORK

Future work in robot safety for the FTS program fits into three general categories: real time world models for dynamic environments, responses to dangerous situations, and fundamental safety issues.

### 3.4.1 Real Time World Models for Dynamic Environments

The FTS program presents some difficult safety problems, primarily due to the dynamic environment in which the FTS robot functions. The environment is dynamic in two ways. First, the robot is not fixed in a single location containing fixed objects, but will be mounted at different locations on the Space Station. Furthermore, objects may move around in the robot's work space at any given location. This highly dynamic environment requires that the robot's world model be updated in real time.

The primary problem in updating the FTS's world model in real time is sensing. The FTS system will need to accurately sense the location of all objects, including inanimate objects and EVA astronauts, in its work space in real time. The sensing of inanimate objects can be achieved through integration of vision, ranging and tactile sensors. There is currently research work being done with all of these sensors[22,24,25] and in multiple sensor integration.[31] Much of this information will apply to the space use of these sensors. While the sensing of humans in the work space is a difficult problem on Earth, it is easier to solve in space, because transmitters and sensors can be incorporated into the space suits that EVA astronauts must wear.

These developments in the research of individual sensors and in multiple sensor integration can be used by FTS system designers to assess the FTS's intrinsic level of safety.

### 3.4.2 Response to Dangerous Situations

Section 3.3.1 discussed the developments required to assess the current safety status of the FTS in the dynamic space environment. Once the environmental information is evaluated, the safety (or danger) of the current situation can be assessed. This in turn may require corrective actions. Appropriate corrective actions may be shutting down or reducing the speed of the robot, or modifying the planned path of the manipulators or the planned series of operations. The primary area that requires work here is modification of the planned path or series of operations. Research is currently being conducted in path planning for collision avoidance in off-line applications. The FTS, however, will require real time path planning, where the primary problem in implementation is ensuring sufficiently fast computational speed.

Also in this category, new hardware may be required for kinetic energy dissipation. It is first necessary to determine whether devices are available that can rapidly stop the robot in an emergency and reduce the damage when a collision occurs. They must also be appropriate for the space application. If none exist, new devices specific to the FTS application may be needed.

Developments of the technology discussed in this section and section 3.4.1 will result in a system capable of detecting a dangerous situation and making the appropriate corrective action.

### 3.4.3 Fundamental Safety Issues

The safety of the FTS system depends on two factors: the system must be designed to be intrinsically safe, and a auxiliary safety computer system needs to be implemented. Much of the work presented in this chapter has focused on designing the system to be intrinsically safe. This study showed that the current understanding of how to make systems safe is crude at best.

The state of the art in designing safe systems is checklists. The checklist presented here for the FTS system (which can also be applied to other autonomous space systems) represents a first step in designing safety into an autonomous system. However, what is really needed is a design evaluation tool that quantitatively assesses the safety of a design.

A similar approach is desperately needed for the auxiliary safety system, to assess the safety of its current state and its planned sequence of operations. This need will increase as we move towards higher levels of automation. The investigators at Rensselaer Polytechnic Institute are currently initiating research into the development of safety assessment tools for use in evaluating designs and in auxiliary safety systems.

## 3.5 REFERENCES

1. Altamuro, V.M. "Working Safely with the Iron Collar Worker," *National Safety News*, July 1983. Reprinted on pp. 73-75 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.
2. Sugimoto, N. and K. Kawaguchi,. "Fault-Tree Analysis of Hazards Created by Robots," *13th International Symposium on Industrial Robots and Robots 7*, April 1983. Reprinted on pp. 83-100 of *International Trends in Manufacturing Technology: Robot Safety*, Bonney, M.C. and Y.F. Yong, Editors, IFS Publications, Ltd., Springer-Verlag, 1985.
3. Carlsson, J. "Robot Accidents in Sweden," Report published by Arbetarskyddsstyrelsen, National Board of Occupational Safety and Health, Sweden, 1984. Reprinted on pp. 49-64 of *International Trends in Manufacturing Technology: Robot Safety*, Bonney, M.C. and Y.F. Yong, Editors, IFS Publications, Ltd., Springer-Verlag, 1985.
4. Sugimoto, N. "Systematic Robot-Related Accidents and Standardisation of Safety Measures," First presented at the 14th International Symposium on Industrial Robots, 2-4 October 1984, Gothenburg, Sweden. Reprinted on pp. 23-29 of *International Trends in Manufacturing Technology: Robot Safety*, Bonney, M.C. and Y.F. Yong, Editors, IFS Publications, Ltd., Springer-Verlag, 1985.
5. "Study on Accidents Involving Industrial Robots," Occupational Safety and Health Department, Tokyo, Japan, August 1983. Translation of *Robotics Report No. 5*, Ministry of Labor, Tokyo, February 1983, 14p.

6. Becker, S. "Development of Mechanical Performance Standards for Robots," *Proceedings of The Workshop on Robot Standards*, June 1985, pp. 141-144.
7. Bloodgood, J. "An Overview of Standards Development for Robots and Robot Systems," *Proceedings of The Workshop on Robot Standards*, June 1985, pp. 1-5.
8. Bloodgood, J. "Survey on Robot Standards," *Proceedings of The Workshop on Robot Standards*, June 1985, pp. 47-57.
9. Lauck, K.E. "Development of a Robot Safety Standard," *Working Safely with Industrial Robots*, Strubhar, P.M., Editor , Robotics International of SME, 1986, pp. 227-233.
10. Ottinger, L.V. and R.N. Stauffer. "Update on Robotic Standards Development," *Robotics Today*, October 1983. Reprinted on pp. 237-241 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.
11. Prange, J.M. and J.A. Peyton. "Standards Development," *Robotics Today*, December 1986, pp. 23-24.
12. Percival, N. "Safety Standards in Robotics," First presented at the Robot Safety Seminar (Univ. Nottingham/ Ford Motor Co.), updated March 1985. Reprinted on pp. 17-21 of *International Trends in Manufacturing Technology: Robot Safety*, Bonney, M.C. and Y.F. Yong, Editors, IFS Publications, Ltd., Springer-Verlag, 1985.
13. Akeel, H.A. "Hardware for Robotic Safety Systems," Tower Conference Management Company's Second Annual International Robot Conference, October 1984, pp. 67-74.
14. Akeel, H.A. "Intrinsic Robot Safety," *Proceedings of the Conference on Robotic Safety*. Reprinted on pp. 61-68 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor.
15. Bellino, J.P. "Design for Safeguarding," *RIA Robot Safety Seminar*, November 1984. Reprinted on pp. 127-132 of *International Trends in Manufacturing Technology: Robot Safety*, Bonney, M.C. and Y.F. Yong, Editors, IFS Publications, Ltd., Springer-Verlag, 1985.
16. Jones, R. and S. Dawson."The Role of Hardware, Software and People in Safeguarding Robot Production Systems," *Proceedings of the 15th International Symposium on Industrial Robots*, Vol. 2, Sept 1985, pp. 557-568.
17. Leipold, F.P. "Robot Construction (Safety Considerations)," *RIA Robot Safety Seminar Proceedings*, 1985, pp. 38-43.
18. Linger, M.., H. Sjostrom, and G. Palmers. "How to Design Safety Functions in the Control System and for the Grippers of Industrial Robots," *Proceedings of the 15th International Symposium on Industrial Robots*, Vol. 2, Sept 1985, pp. 569-577.
19. Barrett, R.J. "Robot Safety and the Law," *Robot Safety Seminar*, November 1982. Reprinted on pp. 3-16 of *International Trends in Manufacturing Technology: Robot Safety*, Bonney, M.C. and Y.F. Yong, Editors, IFS Publications, Ltd., Springer-Verlag, 1985.
20. Bellino, J.P. "Safety Considerations for Robotic Installations," *RIA Robot Safety Seminar Proceedings*, 1985, pp. 44-52.
21. "Photoelectric Guarding," Internal report prepared by Manufacturing Safety Coordination, Ford of Europe, January 1985. Reprinted on pp. 199-204 of *International Trends in Manufacturing Technology: Robot Safety*, Bonney, M.C. and Y.F. Yong, Editors, IFS Publications, Ltd., Springer-Verlag, 1985.
22. "Sensors for Robot Safety," *Robotics World*, May 1983, pp. 16-19.
23. Irwin, C.T. and D.O. Caughman. "Intelligent Robotic Integrated Ultrasonic System," *Proceedings of Robots 9 Conference*, Vol. 2, June 1985, pp. 19-38 to 19-47.
24. Kilmer, R.D.,"Safety Sensor Systems," *Robots VI Conference*, March 1982. Reprinted on pp. 223-236 of *International Trends in Manufacturing Technology: Robot Safety*, Bonney, M.C. and Y.F. Yong, Editors, IFS Publications, Ltd., Springer-Verlag, 1985.
25. McArthur, G.R. "Robot Sensors and Safety with Sensors," *Proceedings of Robots 9 Conference*, Vol. 1, June 1985, pp. 11-97 to 11-103.
26. Harless, M.and M. Donath. "An Intelligent Safety System for Unstructured Human/Robot Systems," *Proceedings of Robots 9 Conference*, Vol. 2, June 1985, pp. 19-9 to 19-20.
27. Derby, S., J. Graham, and J. Meagher. "A Robot Safety and Collision Avoidance Controller," *Proceedings of the Robots 8 Conference*, Vol. 2, June 1984, pp. 21-33 to 21-41.
28. Graham, J.H., J.F. Meagher, and S.J. Derby."A Safety and Collision Avoidance System for Industrial Robots," *IEEE Transations on Industrial Applications*, Vol. IA-22, No. 1, January/February 1986, pp. 195-203.
29. Millard, D. "Robot Safety Research at RPI: A Compilation," June 1986. Available upon request from Rensselaer.
30. Kilmer, R.D. McCain, H.G., Juberts, M., Legowik, S.A., "Watchdog Safety Computer Design and Implementation," *Proceedings of the RI/SME Robots 8 Conference*, June 1984. Reprinted on pp. 101-117 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

31. "Workshop on Multisensor Integration in Manufacturing Automation," Technical Report of the Department of Computer Science, University of Utah: Salt Lake City, Utah, February 1987.

## BIBLIOGRAPHY

Ackerson, D. S. and D.R. Harry. "Theory, Experimental Results and Recommended Standards Regarding the Static Positioning and Orienting Precision of Industrial Robots," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 125-140.

Akeel, H,A. "Intrinsic Robot Safety," Proceedings of the Conference on Robotic Safety, 1983. Reprinted on pp. 61-68 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Akeel, H.A. "Hardware for Robotic Safety Systems," Tower Conference Management Company's Second Annual International Robot Conference, October 1984, pp. 67-74.

Altamuro, V.M. "Working Safely with the Iron Collar Worker," *National Safety News*, July 1983. Reprinted on pp. 73-75 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

American National Standard for Industrial Robots and Robot Systems - Safety Requirements," American National Standards Institute, Inc., ANSI/RIA R15.06-1986, June 13, 1986.

Barcheck, C.A.T. "Methods for Safe Robotic Start-up, Testing, Insepection and Maintenance," *RIA Robot Safety Seminar Proceedings*, 1985, pp. 67-73.

Barrett, R.J. "Robot Safety and the Law," *International Trends in Manufacturing Technology: Robot Safety*, pp. 3-16, IFS Ltd., Springer-Verlag, 1985.

Becker, S. "Development of Machanical Performance Standards for Robots," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 141-144.

Bellino, J.P. "Design for Safeguarding," *International Trends in Manufacturing Technology: Robot Safety*, pp. 127-132, IFS Ltd., Springer-Verlag, 1985.

Bellino, J.P. "Safety Considerations for Robotic Installations," *RIA Robot Safety Seminar Proceedings*, 1985, pp. 44-52.

Bloodgood, J."An Overview of Standards Development for Robots and Robotic Systems," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 1-33.

Bloodgood, J. "Survey on Robot Standards," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 47-57.

Blume, C., B.J. Frommherz, and U. Rembold. "The Proposed Robot Saftware Interfaces SRL and IRDATA," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 74-83.

Bonfioli, M, C.F. Marcolli, and C. Noe. "Safety System Proposal for Automated Production". *International Trends in Manufacturing Technology: Robot Safety*, pp. 101-116, IFS Ltd., Springer-Verlag, 1985.

Bowman, D. "OSHA'S Tinman," SME WESTEC Conference, March 1976. Reprinted on pp. 56-57 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor.

Carlsson, J. "Robot Accidents in Sweden," *International Trends in Manufacturing Technology: Robot Safety*, pp. 49-64, IFS Ltd. , Springer-Verlag, 1985.

Carrico, L.R. "Training and Design for Safe Implementation of Industrial Robots," *International Trends in Manufacturing Technology: Robot Safety*, pp. 169-177, IFS Ltd., Springer-Verlag, 1985.

Carrico, L.R. "A Comprehensive Approach to a Safe Implementation of Industrial Robots". Presented at RI/SME's Robotic Education and Training: Meeting the Educational Challenge Conference, August 1984. Reprinted on pp. 214-223 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Collins, J.W. "Hazard Prevention in Automated Factories," *Robotics Engineering*, July 1986, pp. 8-11.

Colson, J.C. and N.D. Perreira. "The Need for Performance Measures for Robotic Systems and Some Qualitative Definitions," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 145-151.

Colson, J.C. and N.D. Perreira. "Experimental Procedures and Statistics for Determining Parameters of Robotic Systems," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 152-160.

Cook, B.A. "Increased Hardware Safety Margin Through Software Checking," *International Trends in Manufacturing Technology: Robot Safety*, pp. 161-168, IFS Ltd., Springer-Verlag, 1985.

Courter, E. "Toward Safer Robots," pp. 234-236, *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Cox, J.L. and J.K. Butler. "Human Factors Issues in Robotics: Physical, Mental, Safety, Legal," RI/SME AUTOMACH Australia '84 Conference, May 1984. Reprinted on pp. 34-45 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Dagalakis, N. and D. Myers."Use of Correlation Analysis for the Evaluation and Adjustment of Robot Gear Performances," *Proceedings of the Workshop on Robot Standards,* June 1985, pp. 112-118.

DeGregoria, J.P. "Robot Safety: An Overview of the Multiple Risks," LabData, Vol 14, No. 1. Reprinted on pp. 9-12 of *Working Safely with Industrial Robots,* Strubhar, P.M., Editor, Robotics International of SME, 1986.

Derby, S., J. Graham, and J. Meagher. "A Robot Safety and Collison Avoidance Controller," *International Trends in Manufacturing Technology: Robot Safety,* pp. 237-246, IFS Ltd., Springer-Verlag, 1985.

Derby, S., J. Graham, and J. Meagher. "A Robot Safety and Collision Avoidance Controller," Proceedings of the Robots 8 Conference, Vol. 2, June 1984, pp. 21-33 to 21-41. Reprinted on pp. 133-141 of *Working Safely with Industrial Robots,* Strubhar, P.M., Editor, Robotics International of SME, 1986.

Fitzgerald, M.L. and A. Barbera. "A Low-Level Control Interface for Robot Manipulators," *Proceedings of the Workshop on Robot Standards,* June 1985, pp. 58-70.

Gage, D.W., S.Y.Harmon, W.A. Aviles, and G.L. Bianchini. "Subsystem Interfaces for Complex Robots," *Proceedings of the Workshop on Robot Standards,* June 1985, pp. 119-124.

Ghosh, K. and C. Lemay. "Man/Machine Interactions in Robots and Their Effect on the Safety of the Workplace," *Proceedings of Robots 9 Conference,* Vol. 2, June 1985, pp. 19-1 to 19-8.

Graham, J. H., J.F. Meagher, and S.J. Derby. "A Safety and Collision Avoidance System for Industrial Robots," *IEEE Transations on Industrial Applications,* Vol. IA-22, No. 1, January/February 1986, pp. 195-203.

Graham, M.E.K. "Safety Mats," *International Trends in Manufacturing Technology: Robot Safety,* pp. 205-216, IFS Ltd., Springer-Verlag, 1985.

Grossman, D. "AML as a Plant Floor Language," *Proceedings of the Workshop on Robot Standards,* June 1985, pp. 71-73.

Harless, M. and M. Donath. "An Intelligent Safety System for Unstructured Human/Robot Systems," *Proceedings of Robots 9 Conference,* Vol. 2, June 1985, pp. 19-9 to 19-20.

Henkel, S.vL. "Robots and Safety: An Industry Overview," *Robotics Age,* July 1985, pp. 26-28.

Howard, J.M. "Focus on the Human Factors in Applying Robotic Systems," Robotics Today, December 1982. Reprinted on pp. 31-33 of *Working Safely with Industrial Robots,* Strubhar, P.M., Editor, Robotics International of SME, 1986.

Hulfachor, R. "Safety Considerations and Robotic Welding," *Robotics Today,* February 1987, pp. 24-26.

Hunt, G. and J. Tomlison. "EIA Project 1393 A High Level Communciations Standard," *Proceedings of the Workshop on Robot Standards,* June 1985, pp. 34-46.

Irwin, C.T. and D.O. Caughman. "Intelligent Robotic Integrated Ultrasonic System," *Proceedings of Robots 9 Conference,* Vol. 2, June 1985, pp. 19-38 to 19-47.

Irwin, R.D. "Get the Most from Computerized Steel-Collar Workers," Production Engineering, August 1981. Reprinted on pp. 23-27 of *Working Safely with Industrial Robots,* Strubhar, P.M., Editor, Robotics International of SME, 1986.

Jones, D.B. "Human Factors Aspects of Robotic Safety," *RIA Robot Safety Seminar Proceedings,* 1985, pp. 74-78.

Jones, D.H. "An Insight to Robotic Controllers and Servo Systems," Tower Conference Management Company's First Annual International Robot Conference, June 1983. Reprinted on pp. 17-22 of Working *Safely with Industrial Robots,* Strubhar, P.M., Editor, Robotics International of SME, 1986.

Jones, R. and S. Dawson. "People and Robots: Their Safety and Reliability," *International Trends in Manufacturing Technology: Robot Safety,* pp. 65-82, IFS Ltd., Springer-Verlag, 1985.

Jones, R. and S. Dawson. "The Role of Hardware, Software and People in Safeguarding Robot Production Systems," *Proceedings of the 15th International Symposium on Industrial Robots,* Vol. 2, Sept 1985, pp. 557-568.

Kehoe, E.J. "Practical Robot Safety," *Robotics Today,* April 1985, pp. 38-41.

Kilmer, R.D. "Safety Sensor Systems," *International Trends in Manufacturing Technology: Robot Safety,* pp. 223-236, IFS Ltd., Springer-Verlag, 1985.

Kilmer, R.D. "Safety Sensor Systems for Industrial Robots.," Presented at the RI/SME Robots VI Conference, March 1982. Reprinted on pp. 142-153 of *Working Safely with Industrial Robots,* Strubhar, P.M., Editor, Robotics International of SME, 1986.

Kilmer, R.D., H.G. McCain, M. Juberts, and S.A. Legowik. "Watchdog Safety Computer Design and Implementation," Presented at the RI/SME Robots 8 Conference, June 1984. Reprinted on pp. 101-117 of *Working Safely with Industrial Robots,* Strubhar, P.M., Editor, Robotics International of SME, 1986.

Kilmer, R.D., H.G. McCain, M. Juberts, and S.A. Legowik. "Safety Computer Design and Implementation," *International Trends in Manufacturing Technology: Robot Safety,* pp. 141-160, IFS Ltd., Springer-Verlag, 1985.

Kotttke, Thienemann, and Zeich, "User Requirements for a Standardized Robot Language," *Proceedings of the Workshop on Robot Standards,* June 1985, pp. 91-95.

Kulvin, B.F. "How to Safeguard Welding Robots," *Welding Design and Fabrication*, May 1985, pp. 72-75.

Lau, K., L. Haynes, and R. Hocken. "Robot End Point Sensing Using Laser Tracking System," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 104-111.

Lauck, K.E. "Safeguarding of Industrial Robots," pp. 87-97, *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Lauck, K.E. "Development of a Robot Safety Standard," RIA Robot Safety Seminar Proceedings, 1985, pp. 5-12. Reprinted on pp. 227-233 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Leipold, F.P. "Robot Installation Safety Considerations," Proceedings of the Conference on Robotic Safety, 1983. Reprinted on pp. 171-177 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Leipold, F.P.,"Robot Construction (Safety Considerations)," RIA Robot Safety Seminar Proceedings, 1985, pp. 38-43. Reprinted on pp. 195-198 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Linger, M. "Design of Safety Systems for Human Protection," *International Trends in Manufacturing Technology: Robot Safety*, pp. 117-126, IFS Ltd., Springer-Verlag, 1985.

Linger, M., H. Sjostrom, and G. Palmers. "How to Design Safety Functions in the Control System and for the Grippers of Industrial Robots," *Proceedings of the 15th International Symposium on Industrial Robots*, Vol. 2, Sept 1985, pp. 569-577.

Lodge, J.E. "How to Protect Robot Maintenance Workers," National Safety News, June 1984. Reprinted on pp. 178-181 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

McArthur, G.R. "Robot Sensors and Safety with Sensors," *Proceedings of Robots 9 Conference*, Vol. 1, June 1985, pp. 11-97 to 11-103.

Millard, D. "Robot Safety Research at RPI: A Compilation," June 1986, available from the Center for Manufacturing Productivity and Technology Transfer, Rensselaer Polytechnic Institute, Troy, NY, 12180-5390.

Moore, C. "Robot Safety Training for Oldsmobile Employees," *RIA Robot Safety Seminar Proceedings*, 1985, pp. 13-27.

Mohri, S. et al. "Robot Language from Standpoint of FA System Development — An Outline of FA-BASIC," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 161-174.

Morris, H. M. "Making Robots Safe," *Control Engineering*, April 1986, pp. 130-131.

Morgan, D.J. "Safety Considerations in Robot Welding Operations," National Safety News, July 1984. Reprinted on pp. 82-86 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Nicolaisen, P. "Occupational Safety and Industrial Robots," *International Trends in Manufacturing Technology: Robot Safety*, pp. 33-48, IFS Ltd., Springer-Verlag, 1985.

Ottinger, L.V. and R.N. Stauffer. "Update on Robotic Standards Development," *Robotics Today*, October 1983. Reprinted on pp. 237-241 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Percival, N. "Safety Standards in Robotics," *International Trends in Manufacturing Technology: Robot Safety* pp. 17-22, IFS Ltd., Springer-Verlag, 1985.

"Photoelectric Guarding," Manufacturing Safety Coordination (Ford of Europe, UK), *International Trends in Manufacturing Technology: Robot Safety*, pp. 199-204, IFS Ltd., Springer-Verlag, 1985.

Powel, A.B. "Robot Nomenclature, Operation and Applications," Proceedings of the Conference on Robotic Safety, 1983. Reprinted on pp. 3-8 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Powis, B. "Perimeter Guarding," *International Trends in Manufacturing Technology: Robot Safety*, pp. 217-222, IFS Ltd., Springer-Verlag, 1985.

Prange, J.M. and J.A. Peyton., "Standards Development," *Robotics Today*, December 1986, pp. 23-24.

Ramirez, C.A. "Artificial Intelligence Applied to Robot Fail Safe Operations," *Proceedings of RI/SME Robots 9 Conference, Vol. 2, June 1985, pp. 19-21 to 19-36. Reprinted on pp. 154-168 of Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Ramirez, C.A. "Robot Intelligent Safety System," *Proceedings of Robots 9 Conference*, Vol. 2, June 1985, pp. 19-50 to 19-62.

Reader, D.E. "Human Factors in Automation," *Manufacturing Engineering*, October 1982. Reprinted on pp. 46-48 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Robinson, O.F. "Robot Guarding - The Neglected Zones," *International Trends in Manufacturing Technology: Robot Safety*, pp. 181-188, IFS Ltd., Springer-Verlag, 1985.

Sato, Y. and K. Inoue. "Safety Assessment of Human-Robot Systems (First Report, Hazard Identification Based on the Action-changes and Action-Chain Models), *Bulletin of JSME*, Vol. 29, No. 250, April 1986, pp. 1356-1361.

Sato, Y., K. Inoue, and H. Kumamoto. "The Safety Assessment of Human-Robot Systems (Second Report, Logic Models for the Analysis of the Accident Causing Mechanisms-Part 1), *Bulletin of JSME*, Vol. 29, No. 256, October 1986, pp. 3618-3625.

Schreiber, R.R. "Robot Safety: A Shared Responsibility," *Robotics*, Oct 1983, pp. 60-65.

"Sensors for Robot Safety," *Robotics World*, May 1983, pp. 16-19.

Spur, G., F.-L.Krause, and R. Dassler. "CAD — Systems for Off-Line Programming as an Objective for Standardization," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 96-103.

Stauffer, R.N. "Motion Control of Automation Equipment," *Robotics Today*, June 1983. Reprinted on pp. 13-16 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Strubhar, P. "Robotic Safeguarding," *RIA Robot Safety Seminar Proceedings*, 1985, pp. 28-37.

"Study of Accidents Involving Industrial Robots," Occupational Safety and Health Department, Tokyo, Japan, August 1983.

Sugimoto, N. "Systematic Robot-Related Accidents and Standardisation of Safety Measures". *International Trends in Manufacturing Technology: Robot Safety*, pp. 23-29, IFS Ltd., Springer-Verlag, 1985.

Sugimoto, N. and K. Kawaguchi. "Fault-tree Analysis of Hazards Created by Robots," *International Trends in Manufacturing Technology: Robot Safety*, pp. 83-98, IFS Ltd., Springer-Verlag, 1985.

Sugimoto, N. and K. Kawaguchi. "Fault Tree Analysis of Hazards Created by Robots," Presented at the RI/SME 13th ISIR/Robots 7 Conference, April 1983. Reprinted on pp. 118-132 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Sugimoto, N. and K. Fukaya. "Safety of Teaching by Off-Line Teaching," *Proceedings of the 15th International Symposium on Industrial Robots*, Vol. 2, Sept 1985, pp. 579-586.

Thompson, C. "Safety Interlock Systems," *International Trends in Manufacturing Technology: Robot Safety*, pp. 189-198, IFS Ltd., Springer-Verlag, 1985.

Traue, E., M. Weck, and T. Niehaus. "An Industrial Robot Controller Equipped with the IRDATA-Interface for Off-Line Robot Programing," *Proceedings of the Workshop on Robot Standards*, June 1985, pp. 84-90.

Trouteaud, R.R. "Safety, Training and Maintenance: The Influence on the Success of Your Robot Application". Presented at the SME Robots IV Conference, October 1979. Reprinted on pp. 182-194 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Weatherby , V. and S.A.R. Pike. "The Safety Implications of a New Technology," *Industrial Robot*, Vol 10, No. 3 (September 1983), pp. 185-188. Reprinted on pp. 69-72 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Willson, R.D. "How Robots Save Lives!," RI/SME Robots VI Conference, March 1982. Reprinted on pp. 49-55 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Wisniewski, G.R. "Robot Training in the Automotive Industry," *Proceedings of the Conference on Robotic Safety*, 1983. Reprinted on pp. 201-213 of *Working Safely with Industrial Robots*, Strubhar, P.M., Editor, Robotics International of SME, 1986.

Yong, Y.F., N.K. Taylor, and M.C. Bonney. "CAD - An Aid to Robot Safety System Design," *International Trends in Manufacturing Technology: Robot Safety*, pp. 133-140, IFS Ltd., Springer-Verlag, 1985.

"Workshop on Multisensor Integration in Manufacturing Automation," Technical Report of the Department of Computer Science, University of Utah: Salt Lake City, Utah, February 1987.

Ziskovsky, J.P. "Risk Analysis and Safeguarding of Robotic Applications," *RIA Robot Safety Seminar Proceedings*, 1985, pp. 53-66.

Ziskovsky, J.P. "Risk Analysis and the R3 Factor," *Proceedings of the Robots 8 Conference*, Vol. 2, June 1984, pp. 15-9 to 15-13.

# 4.0 HUMAN PERFORMANCE CONSIDERATIONS

Dr. George V. Kondraske
Ms. Katy Hoard

The Human Performance Institute
The University of Texas at Arlington

## 4.1 INTRODUCTION

The flight telerobotics system (FTS) will play a major role in realizing implementation of the space station. Due to the sophistication of this system and the nature of the task and environment in which it will operate, there are a number of areas worthy of special safety considerations. As part of a four university team under contract to Goddard Space Flight Center through the Consortium for Space/Terrestrial Automation and Robotics (C-STAR, a Division of Universities Space Research Association), the Human Performance Institute at the University of Texas at Arlington is investigating *human performance* issues that can impact safety. This document represents a final report of our work and addresses two primary situations:

1. the human-telerobotic workstation interface
2. extravehicular (EVA) situations in which astronauts and the telerobot operate close together.

### 4.1.1 Assumptions

In focusing energies and attention on the issue of safety toward a complex engineering system such as the FTS, the easy task is to identify possible sources of concern. This is especially true given the freedom to postulate any of a number of hypothetical scenarios. The more difficult task is to weigh the likelihoods and risk exposures toward identification of *generalizable* safety concerns and propose methods for their strategic management.

The *assumptions* are an essential component in safety-oriented investigations. In consideration of human performance related issues and the FTS, the following points are considered relevant in the context of assumptions:

- While scenarios that raise great concern can be postulated, many represent highly improbable events.

- The humans involved (astronauts) are highly trained with great capacity to work accurately and reliably under demanding circumstances. (*Note*: this assumption should be reconsidered if mission specialists, e.g., scientists, are anticipated to interface with the FTS.)

- At the current time, and for the foreseeable future, it is not possible to monitor and protect every aspect of an environment for every situation by *technological means*. Ironically, an overabundance of such artifical mechanisms can result in a false sense of security in the humans they are intended to protect. That is, humans require a certain amount of "tension" in the environment to maintain a level of alertness and concern for safety issues. *Humans* are the most powerful safety monitors and enhancers available.

- A last assumption is composed of two components:

  1. the FTS is not a completely designed system at this time
  2. the FTS is intended to be an evolutionary system.

These assumptions underlie our investigative approach.

### 4.1.2 Approach

This is not a specific critic-oriented "devil's advocate" safety approach that one can apply to a finalized system. Rather, the approach is to raise general issues toward the ends of:

- incorporating safety-oriented components into the design and implementation processes for a first generation system, and
- maximizing safety over a long-term, multiple generation life cycle.

In addition, it is assumed that NASA already has considerable human factors and safety related reference material, procedures, and standards, one example of which is cited here.[1] Thus, an objective, somewhat speculative approach is taken here to provide, perhaps, some new insights into issues within our scope of investigation. The approach toward human- telerobotic workstation interfaces is to *raise designers' awareness* of workload demands placed on the human operator in terms of his/her *performance resources of various dimensions.*

In general, demands in excess of individual performance resource limitations (especially those within the human central processing domain) can compromise safety. Discussion applies to three types of conditions:

1. autonomous robot operation,
2. semi-autonomous robot operation, and
3. teleoperation.

To investigate key issues for the situation in which the robot and the astronaut are within close proximity, a two part approach is utilized. In part A *(human performance/behavior considerations)*, general scenarios are evaluated in which human performance limitations on the part of the astronaut conducting the EVA or FTS may pose potential safety problems. In part B *(robot safety-oriented "reflex" responses)*, human behavior models related to built in-protective mechanisms are offered. These models provide a basis for considering autonomous robot design which may have the potential to positively impact overall long-term safety of the FTS in both predictable and unanticipated situations.

Individual elements of this safety review are not independent, i.e., considerable overlap and interactions are possible. Discussion of such situations is woven into relevant sections of the report as deemed appropriate.

## 4.2 HUMAN/WORKSTATION INTERFACE

The present preliminary design for the FTS calls for both autonomous and human-controlled operation of the telerobot. With the astronaut in control, a key issue concerns his/her ability to properly execute required operations. The macro task in this case is workstation operation, which can be divided into a number of tasks and subtasks from the human operator's perspective. The general situation is depicted in Figure 4-1 and a simplified model of important components is shown in Figure 4-2.

It is assumed that remote sensory information will be provided to the operator via the FTS components, such as real-time visual display of current action, as well as various FTS status indicators. The operator must:

1. process sensory information in real time to arrive at mental decisions which translate to FTS system "commands," and
2. generate appropriate motor outputs to the workstation to exert control over the FTS.

It is also noted that, based on present design conceptualizations (with the controlling astronaut in a cupola), the workstation operator will have the opportunity for direct visual contact. Thus, two primary sources of information must be considered to determine the operator's processing load.

Literature review of analogous situations (e.g., nuclear reactor control) indicates that most errors that lead to compromised safety are categorized broadly as "human error." No specificity regarding the source of error is usually proposed, but human information processing limitations appear to be a prime contribution.

Typically, as many error checks and safeguards are built into the system being controlled as is practical and/or identifiable during the design process. Extensive training on planned task scenarios and use of high reliability

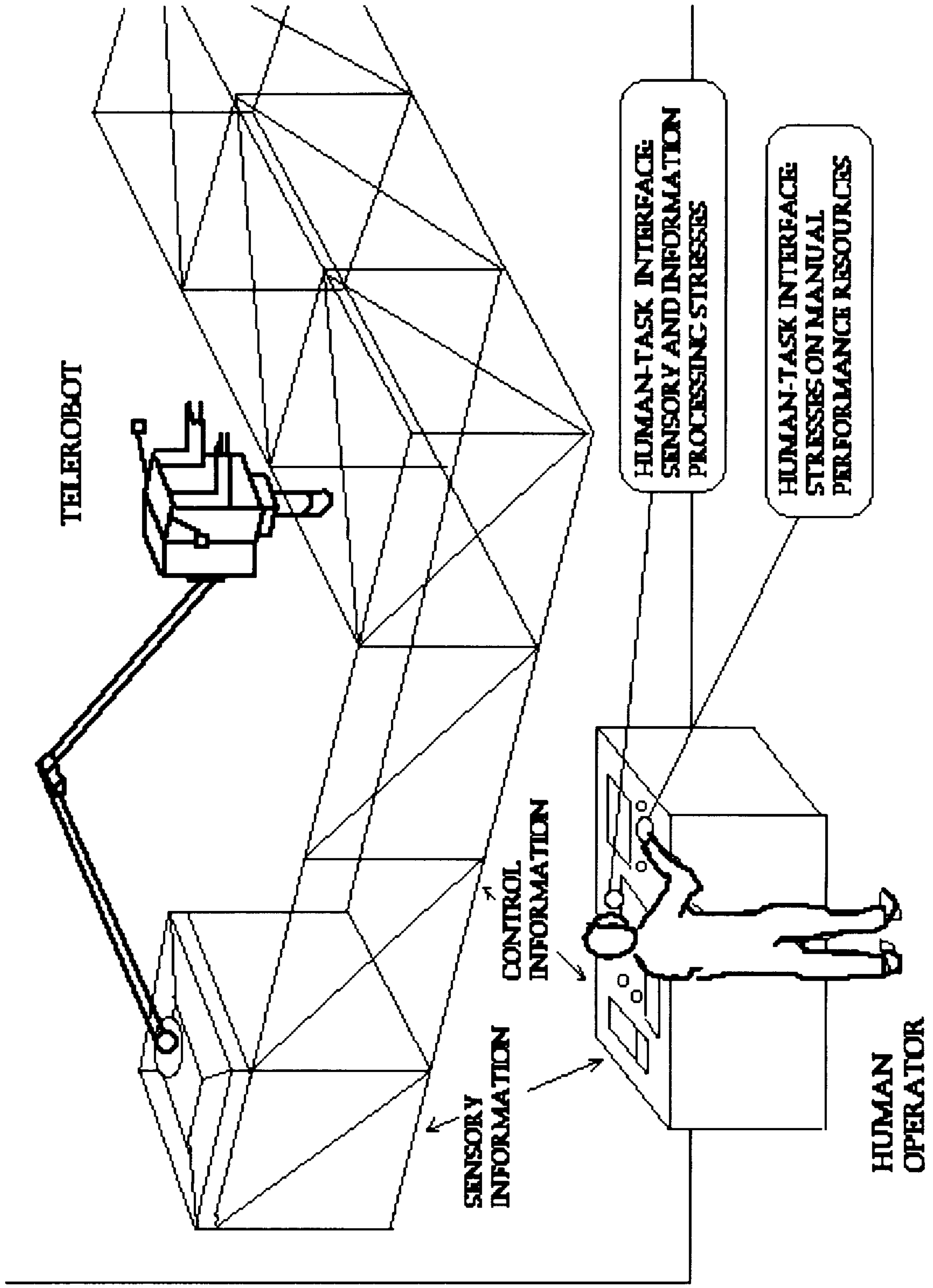

TELEROBOT
HUMAN-TASK INTERFACE: SENSORY AND INFORMATION PROCESSING STRESSES
HUMAN-TASK INTERFACE: STRESSES ON MANUAL PERFORMANCE RESOURCES
CONTROL INFORMATION
SENSORY INFORMATION
HUMAN OPERATOR

FIGURE 1

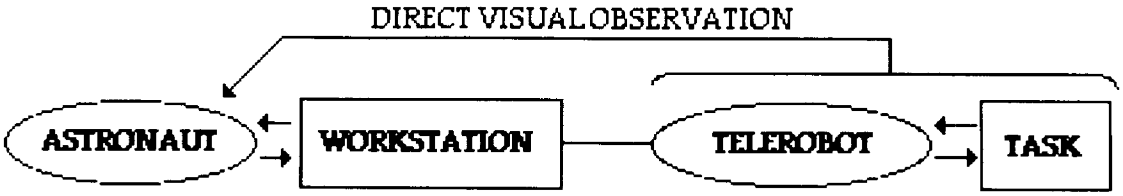


Figure 4-2. Schematic diagram of primary components in FTS system. Information pathways are emphasized.

personnel are the traditional methods used to maximize safety. Thus, reliable and safe operation is expected under the circumstances that are most likely to occur (i.e., those representing identified goals, plans, and conditions) and form the primary basis for system *as well as operations* design.

Further insight can be gained by consideration of a breakdown of the *universe of situations* to which the complete system (operator-robot) is exposed (Figure 4-3). From a design perspective, circumstances that indicate potential safety compromises will *always* be considered less likely and therefore "unusual." A subset of these will usually be anticipated to a degree, but exhaustive consideration is impractical and some situations which may prove "obvious" from hindsight will elude design teams. The subset of conditions which are predicted include both *mission tasks* (primary FTS functions) and certain *safety compromising situations* (those due to human errors, unexpected stresses, or robotic system malfunction). *Predicted* safety compromising situations provide the basis for including special sensors and fail-safe system responses to each sensed condition into the system design. Most technological safety design methods used to date represent this simple Pavlovian approach.

The *remaining subset* of circumstances, which may best be termed "everything else" (such as the need to perform an unexpected task due to a component failure or other reason) are not individually considered in design and training, and therefore require *real-time human judgment*. Such situations may demand execution of tasks which have not been practiced with the FTS system and/or operator, and these may maximally stress the human operator and system in specific ways.

With respect to safety, relatively little effort has been devoted to understanding the human interface to the system - especially in quantitative terms. The NASA document Space Station Man-System Integration Standards[1] was reviewed for guidance. This reference manual documents much useful design information relevant to safety, and we assume that such documents will be standard references for contractors. However, many key aspects are currently covered with a mixture of very subjective terms ("smooth," refresh rates on screens shall be "sufficiently high") and more quantitative criteria ("delay .... shall not exceed 0.1 sec"). For more on this, refer to the document section 9.3.3.4.2, Joysticks. A model for discussion of these aspects of the complete system is deemed appropriate.

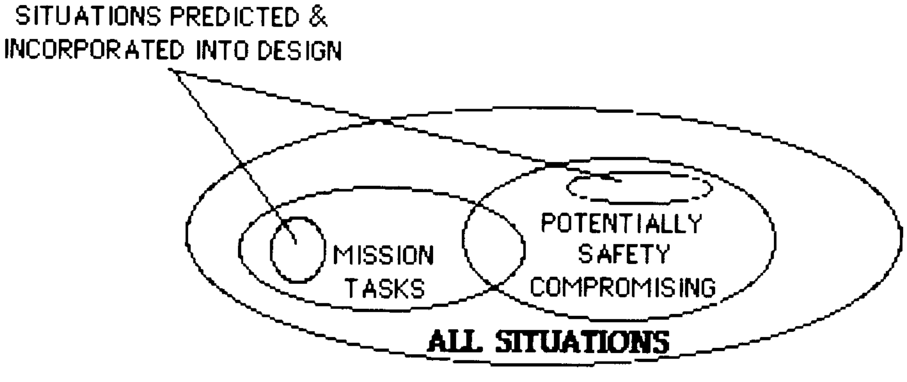


Figure 4-3. Venn diagram dividing situations to be encountered by the FTS system into major subsets from which further subsets are drawn to compose the set of situations referred to as "predicted."

### 4.2.1 Human-Task Interface Conceptual Model

The elemental resource model proposed by Kondraske[2] to help understand human-task interfaces in broad contexts is used. In this model, the human system is divided into three domains: 1) central processing, 2) environmental interface, and 3) life sustaining. Each domain consists of individual subsystems or functional units. Performance of each functional unit is characterized in terms of a multidimensional performance space with dimensions such as speed, memory capacity, strength, etc. Performance is considered to be a collection of elemental resources, such as visual memory capacity, visual information processing speed, or attention. Tasks are modeled and analyzed in terms of the resources required. This model is summarized in Figure 4-4.

In the safety context, the important consideration that results from this model is: **limited availability of any one human performance resource with respect to task demands can prevent the operator from accomplishing a task.**

It is noted that this framework can be applied not only to the human-telerobot workstation interface, but also to the telerobot-task interface.

This resources model implies that at a given system-task interface, the desired design goal is to accomplish the desired task (or class of tasks) while *minimizing the stress across all system performance resources*. It is important to note that this can be achieved either by maximizing the performance resources available, or by designing the task so as to minimize demands placed on the system (the human factors approach). The latter option relates to the design of the FTS workstation and its plan of operation. Minimizing stress on human performance resources (such as information processing capacity or speed) makes available a greater *resource reserve* to deal with the unexpected, increasing the safety margin.

Anticipated tasks and situations, by definition, would be rehearsed on an a priori basis. Training, in effect, reduces the stress on human performance resources - it makes it easier to accomplish a task. Highly autonomous robots can be employed in often-performed tasks, as well as in tasks that are infrequent, but crucial and highly predictable. This reduces opportunities for human-caused hazards. Regardless of the level of autonomy, when planned circumstances and tasks are encountered, neither the resources of the human nor the FTS would be stressed beyond availability. Once this is understood, focus can be directed to two general circumstances:

1. The human operator, for some reason, does not possess the anticipated amounts of performance resources on which the workstation design are based.

2. Circumstances are such that a new task must be accomplished—one which is not within the rehearsed (or autonomous) repertoire of the telerobot-operator combination. In this case, the level of robot autonomy will probably be very low; the operator will be required to assume full control and attempt to plan and execute the task in real-time. Plans may include subtasks that stress performance resources (system and operator) within the bounds of availability. Formulation of such plans represents a complex prediction and many factors may have to be considered.

### 4.2.2 Specific Performance Resource Considerations

It has been noted that any of the many human basic elements of performance which is stressed beyond availability can prevent achievement of the desired goal.

**Life-sustaining Resources.** Cardio-respiratory, renal, and other major systems must provide an adequate supply in order not to affect performance in the central processing and environmental interface (sensory-motor) domains of the human system. It is anticipated that variables which reflect status of these functions will be monitored by life support systems, providing at least the opportunity to consider an input link to FTS fail-safe systems.

**Environmental Interface Resources.** Each sensory-motor unit (muscle and proprioceptive feedback) and sensor (eyes, ears, tactile sensors) of the human body may be involved, depending on the task. Dimensions of performance that must be considered are summarized in Table 4-1.

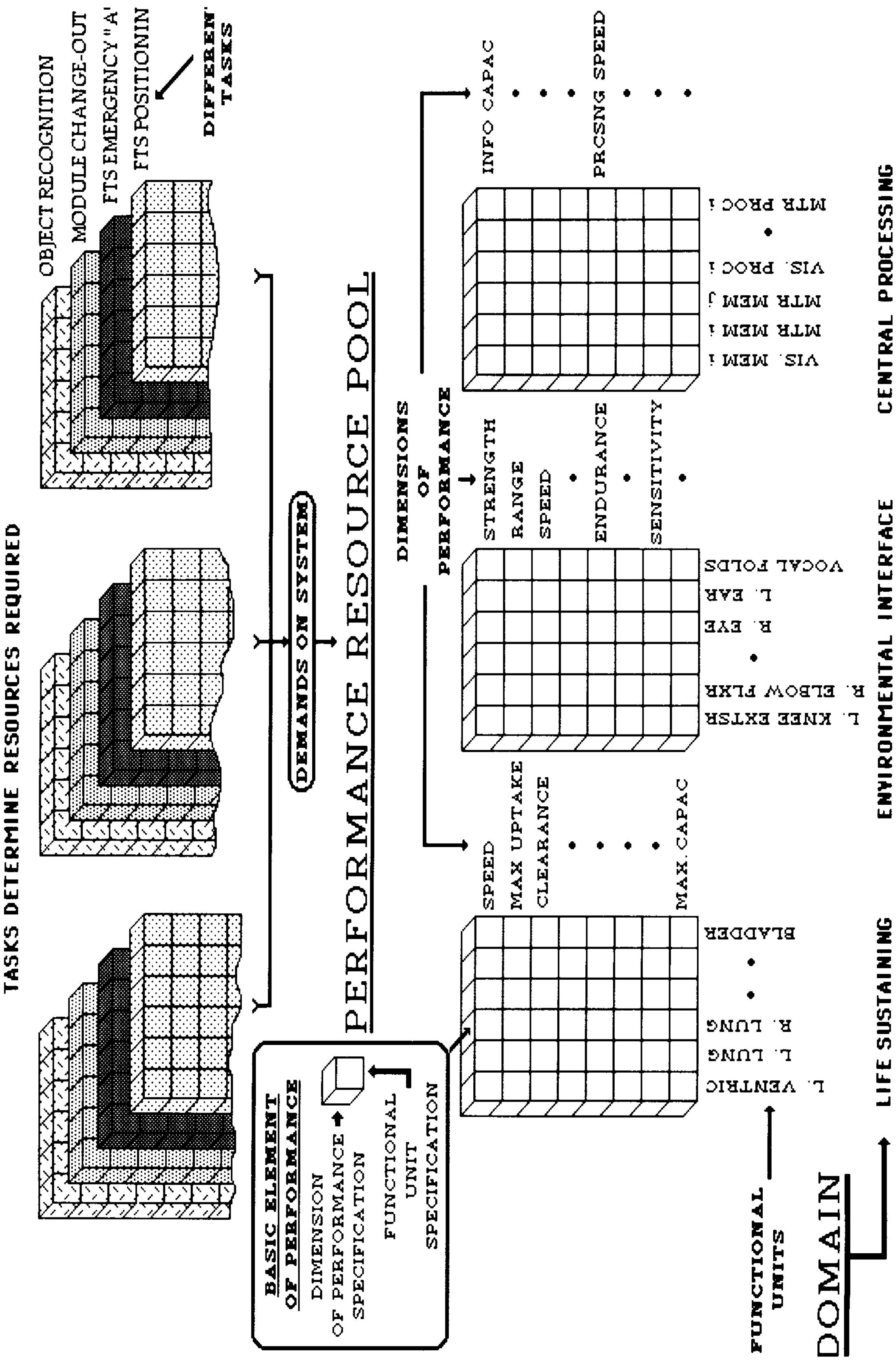


Figure 4. Elemental Resource Model for Human-Task Interface

Table 4-1. **Dimensions of performance associated with types of major functional units in the environmental-interface domain of the human system.**

| Unit Type | Dimensions of Performance |
|---|---|
| Sensory-motor | strength (force/torque production) |
| | range of motion |
| | speed (movement) |
| | steadiness |
| | positioning accuracy |
| | endurance |
| Sensors (visual, auditory, tactile) | sensitivity |
| | bandwidth (channel capacity) |

The values of these parameters set limits within which artificial systems must operate. For example, audio warning stimuli must be "loud enough" (which can be expressed quantitatively) to be heard (determined by auditory sensitivity) within the prescribed environment.

**Central Processing Resources.** The central processing domain is modeled in terms of a large set of processing units, communications channel, and memory units. Processors must deal with information received from multiple sensors in parallel. Interprocessor communications is required. Long-term memory is drawn upon to perform learned or "automatic" tasks. Short-term memory is used to save immediate past history, which is important in making decisions related to task planning.

Information processing can be limited in terms of speed and capacity (too much information must be processed simultaneously). The concept of *attention* has been modeled by Navon and Gopher[3] as a central processing resource that must be shared among tasks if the situation demands that multiple tasks be executed in parallel. Attention has received much interest as a limiting factor in overall workload in situations which may be considered analogous to telerobotic operation, such as workload presented to the pilot by the cockpit of a sophisticated military aircraft.[4]

Both the resources available (human) and resources required (for workstation operation) in this domain are difficult to quantify. However, research in this area is intensive.

Table 4-2 summarizes the types of functional units and dimensions of performance which must be considered.

Design efforts should strive to minimize stress on these resources. Further research is required (and highly recommended) to develop more quantitative approaches to task analysis at the human interface level.

Table 4-2. **Dimensions of performance associated with types of major functional units in the central processing domain of the human system.**

| Unit Type | Dimensions of Performance |
|---|---|
| processor | speed |
| | accuracy |
| | input channel capacity |
| | output channel capacity |
| memory | capacity |
| communications channel | capacity |

### 4.2.3 General and Specific Recommendations

Based upon the just-described model and characterizations, the following recommendations are offered:

- Designers should strive to minimize stress across all human performance resources. The elemental resource model can serve as a *checklist* and can be applied subjectively, for instance, by simply asking questions such as "What can I do to reduce the demand on _______ (visual sensitivity, grip strength, information processing capacity." It can also be used in more quantitative form, if appropriate models are developed for simulations.

- Multiple pathways for receipt of the same sensory information should be investigated and perhaps controlled. This will avoid the operator's confusion about frame of reference, as well as potential overload of processing related resources. For example, it may be desirable to prevent the operator's having direct visual contact with the telerobot in addition to input from artificial sensors (video cameras and displays).

- "Smart" technologic systems—those with the capability to respond to combine multiple sensor outputs and arrive automatically at a situationally determined response—could prove beneficial for long-term considerations. (See section 4.3.2, "Robot Design Considerations," for more details).

- Manual control demands placed on the human may be in question in a micro-gravity environment. That is, the human system depends heavily on the sensory input received from the feel of a control. Design should attempt to provide the same feel on earth and in space so that training will effectively be directed toward the same task (as defined by human performance resource requirements).

- Situations that are not predicted on an a priori basis represent the greatest opportunity for risk exposure. Even human operators who are considered to be highly trained will be untrained, and the demands of the robot task, translated to demands on the human system, will be unknown and difficult to predict. That is, it may be easy to underestimate demands relative to performance resource availability. Advanced simulation capabilities, which incorporate estimations of demands on individual human performance resources, would allow experiments with task design to maximize the probability that demands are within the bounds of available resources.

- Levels of robot autonomy should be limited and well-defined to avoid operator confusion regarding responsibility. At the extremes, the human would know that he or she is totally in control or not at all in control (except for the option of taking over totally). In-between states must be well defined.

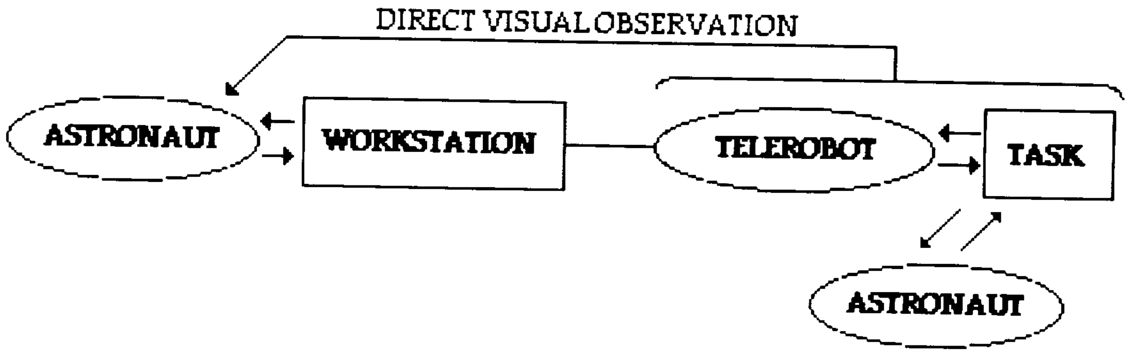


Figure 4-5. Schematic illustration of key components for situation in which the telerobot and astronaut are close together. Two humans and one complex system (FTS) provide multiple degrees of freedom to consider, which place additional demands on communication and information processing.

- Workstation (and overall FTS) design might consider methods to monitor operator performance. Outputs from workstation controls and from the astronaut's life support system could be inputs to a "performance monitoring module" that is part of the FTS. This module would process data according to specified algorithms and generate fail-safe actions if certain predetermined conditions occur.

Safety, related to human control of artificial systems such as robots, will not improve significantly above that now realized in commercial aviation, for example, without the advancement of models to help understand the human processes involved in greater detail.

## 4.3 HUMANS AND TELEROBOT WORKING CLOSE TOGETHER

It is anticipated that an astronaut and the telerobot will co-participate in EVA, and there are obvious safety issues raised. Figure 4-5 schematically summarizes this situation.

Many human performance/task design considerations in this situation are similar in type to those described in more detail under section 4.2, "Human/workstation interface." However, the opportunity for safety compromises is increased since there are now two humans and one complex robot operating to accomplish essentially a common task. The orchestration required is increased and demands on intercommunications among these three primary units are increased, especially if situations should arise that are unpracticed.

Data exist regarding injuries that occur in quasi-analogous industrial robot situations. (Typically a worker is not side by side with a robot during operation, but a situation may arise that causes a human to come close to the robot.)

One generalization appears to emerge. Most injuries seem to be precipitated by some type of robot failure, which at first causes no harm. For example, the robot unexpectedly stops, or appears to be stuck in a position where remote control is difficult to use to correct the situation. A human then decides to intervene mechanically and the robot reacts unexpectedly, resulting in injury. Other situations involve a lack of awareness on the part of the human as to what a robot is doing. This characterization presumes that the responsibility for awareness is *assumed* by the human. However, there are increased trends toward the incorporation of intelligent artificial sensory systems in robots as safeguards. Thermal, video, and force (torque) sensing methods are used, among others.

### 4.3.1 Human (Astronaut) Perspective

From the human perspective, communication is very important. Real-time information as to what the robot is doing is essential. In addition, it is important to know how the robot will react in unconventional situations. In other words, it will be helpful to understand the psyche of the telerobot (to be expanded). A key question is how much information can the astronaut handle. Given finite capacities for information processing, attempts to "over-inform" the astronaut regrading robot status (and plans of the workstation controller) may in fact be a distraction from the astronaut's primary task ("don't bother me now"), which could compromise safety.

On the other hand, the primary task may place such heavy demands on astronaut attention and processing resources that important communications may be ignored. A careful balance regarding planned usage of processing resources is required. Artificial "pre-processors" which monitor the situation (watchdogs) and then alert the astronaut if a specific situation or set of situations are recognized provide the advantage of reducing the average information processing load on the astronaut.

### 4.3.2 Robot Design Considerations

To date, most attempts to incorporate safeguards into robots have relied on purely heuristic approaches. A fundamental problem is the fixed nature of typical fail-safes which are used currently. Frequently only a single variable is sensed (such as position), and if a limit is exceeded a fail-safe action is taken (for instance, STOP). Upon analysis of other information, it may be determined that "stop" is not an optimum response and, in fact, may continue the development of an emerging safety compromise. A better response (e.g., reverse motion) may be possible. Such decisions are frequently made by humans and depend on sufficient sensory information.

This again suggests the need for development of a model. A cybernetic approach can be explored to reveal strategies for incorporating automatic or "reflex" robot reponses. The following is a human behavioral model, which may be beneficial in understanding alternatives to simpler fail-safes.

**Intrinsic Human Safety Reflexes.** A fundamental and well accepted construct of human behavior, and of most living things, is the stimulus-response scenario. That is upon input of sensory information (external or internal, such as an idea), the living system generates a response. This scenario is implemented both consciously and subconsiously. The latter is characterized as a reflex response. Humans are born with and develop a number of such responses which appear to be in place for the primary purpose of self protection.

The process of a human operating in a situation where a danger may occur can be modeled in terms of a multi-dimensional sensory processor consisting of a look-up table. Each sensory channel represents a different dimension in the look-up space. A sample of all sensory channels at a given point in time represents the *stimulus*. The *value* of a given dimension which is sensed can be used to locate a cell in this multi-dimensional space. The cell contains the *response* (stop doing what is now in progress, get out of the way). In humans, past history (training, experience) serves to "fill in the cells" with the optimized or "best" response under the circumstances (characterized by sensory information). Figure 4-6 illustrates this model schematically, which we shall refer to as *situation recognition*.

This model illustrates that flexibility can be incorporated into fail-safe responses and that plans can be made for a variety of such responses (one for every cell in the multi-dimensional sensor space. For instance, as a situation develops, it may become obvious that some damage will be done. Real-time decisions must be made to minimize damage or, in other terms, optimize the response. Under some circumstances, damage to a component should be avoided and a response to achieve this goal would be warranted. However, if the response to avoid component damage would injure an astronaut, it may be warranted to permit the component damage to occur. This could be incorporated into the above situation recognition model with a hierarchical structure to combine multiple sensory dimensions to create a new dimension (such as the probability of astronaut injury). Once again, the value along this dimension can be used to select the response.

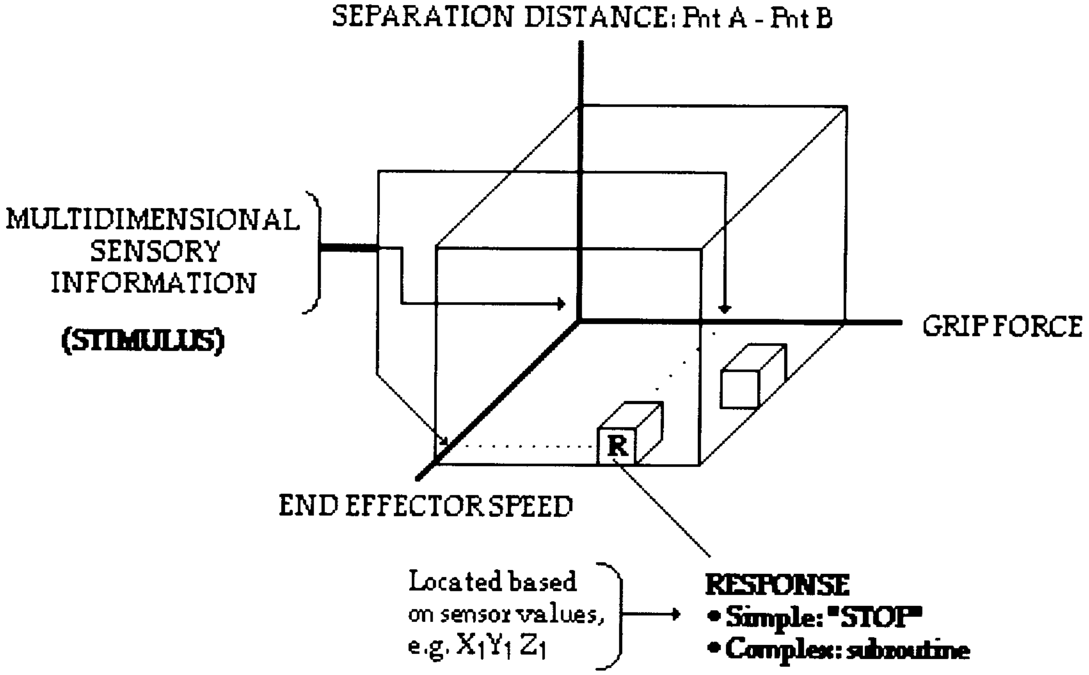

SEPARATION DISTANCE: Pnt A - Pnt B
MULTIDIMENSIONAL SENSORY INFORMATION
(STIMULUS)
GRIP FORCE
R
END EFFECTOR SPEED
Located based on sensor values, e.g. $X_1 Y_1 Z_1$
RESPONSE
• Simple: "STOP"
• Complex: subroutine

Figure 4-6. Schematic representation of situation recognition, as it could be applied to sensed robot variables to generate a wide variety of optimized safety responses.

### 4.3.3 General and Specific Recommendations

Since the general scenario encompasses the human-workstation interface scenario previously considered, recommendations offered for that scenario are generally applicable. In addition, the following points are offered:

- Simulation models will be important in this situation and useful at all stages in FTS life (design, initial test and acceptance, and advanced evolutions).

- Human responses to what would be perceived to be FTS system failures deserve special consideration. Several power-up modes may be warranted to allow recovery from such situations. For example, a "weak and slow" robot mode may allow an astronaut to manually help a manipulator out of a jammed situation while minimizing astronaut jeopardy. Perhaps several programmable levels of robot "strength" and "speed" would be useful.

- Since three units are involved (two astronauts + FTS), it is essential that a single point of control be identified in all tasks. The point of control may be shifted over time (as new subtasks are performed). Such shifts should be adequately communicated and provision for acknowledgment should be incorporated before the next phase or subtask is initiated.

- Incorporation of an artificial speech generator component to the FTS may be beneficial. Tied into autonomous algorithms and the manually operated workstation, the telerobot can take on an additonal human-like character and "announce" completion of subtasks and plans for the next operation. This will facilitate intercommunication, the importance of which for safety cannot be overemphasized.

## 4.4 CONCLUSION

This report attempts to provide a broad perspective on human performance safety issues regarding the FTS. Due to the multitude of scenarios possible with the flexible system, emphasis is placed on generalizeable considerations. Specific recommendations as well as more speculative concepts, based on well-established knowledge and emerging areas, are provided.

Rapid changes are occurring in artificial intelligence and in areas such as neural networks and human behavior modeling. Given that a relatively long life is anticipated for the FTS and given that it is evolutionary in nature, it should be *expected* that significant system changes will be implemented to improve intelligent safety response capability. Setting such expectations early can reduce resistance to changes which in turn will insure that the latest and best options are taken advantage of as soon as possible to enhance safety.

How much safety is enough? This question is especially difficult to answer given a focus on human performance due to current reliance on subjective estimatation. A balanced perspective is required as more quantitative models develop.

## 4.5 REFERENCES

1. *Space Station Man-System Integration Standards* . NASA-STD-3000,Vol.IV, Dec. 18,1986.
2. Bonney, M.C. and Y.F. Yong. *Robot Safety* , IFS Publications, 1985.
3. Navon D., and D. Gopher. "On the Economy of the Human Processing System," *Psych. Rev.* 86, 214-253, 1979.
4. Wickens, C.D., S.J. Mountford, and W.S. Schneider. "Time-Sharing Efficiency: Evidence for Multiple Resources, Task Hemispheric Integrity, and Against General Ability." *Human Factors* 23, 211-229, 1981.

## BIBLIOGRAPHY

Andary, J.F., S.W. Hinbal, J.E. Provost, and J.G. Watzin. The Flight Telerobotic Servicer (FTS): A Focus for Automation and Robotics on the Space Station, *2nd AIAA/NASA/USAF Symposium on Automation, Robotics, and Advanced Computing for the National Space Program,* March, 1987.

Barnes, D.P., N.W. Hardy, and M.H. Lee. "Knowledge Based Error Recovery in Industrial Robots," *Proc. Eighth IJCAI,* Vol.2, pp. 824-826, August 8-12, 1983.

Carlson, J. *Industrial Robots and Accidents at Work* TRITA-A06-0004 (Sweden), 1974.

Collins, J.W. "Safety and Human Factor Considerations in Robotics," *AUTOFACT 1986,* Nov. 12-14, 1986, pp. 3-19 - 3-26.

Dornic, S. and P.M. Rabbitt. *Attention and Performance* , Academic Press, 1975.

Fernandez, K. and E. Hinman. "The Use of a Computer Graphic Simulation in the Development of On-Orbit Tele-Robotic Systems," *Robots 11,* April 26-30, 1987.

*Flight Telerobotic Servicer (FTS) Statement of Work.* RFP5-11381/228, NASA/Goddard Space Flight Center, Greenbelt,MD, May 1,1987.

*Flight Telerobotic Servicer (FTS) Strawman Concept Engineering Report.* SS-GSFC-0031, Goddard Space Flight Center, Greenbelt, MD, March 15,1987.

Fleishman, E.A. and M.D. Dunnette. *Human Capability Assessment* , Lawrence Erlbaum Associates, 1982.

Fleishman, E.A. and M.K. Quaintance. *Taxonomies of Human Performance,* Academic Press, 1984.

*Handbook of Perception and Human Performance,* Vol. I, John Wiley and Sons Ltd., 1986.

Harris, A. *Human Measurement* , Heinemann Educational Ltd., 1978.

Kondraske, G.V. "Looking at Human Performance," ASME *Soma, Engineering for the Human Body* , July 1987.

Kondraske, G.V. "Human Performance: Science or art?" *Thirteenth Northeast Bioengineering Conference, Proceedings,* Phildelphia, pp.44-47, 1987.

Larcombe, M.H.E. and Halsall, J.R. *Robotics in Nuclear Engineering: Computer Assisted Teleoperation in Hazardous Environments* ,Graham and Trotman, 1984.

Maletz, M.C. "An Architecture for Consideration of Multiple Faults," *2nd CAIA,* pp. 267-273, Dec. 5-7, 1984.

*MSFC Software Management and Development Requirements* . (MA-001-006-2E), NASA Marshall Space Flight Center, AL 35812.

*NASA/NBS Standard Reference Model for Telerobot Control System Architecture (NASREM).* SS-GSFC-0027, National Bureau of Standards Robot Systems Division, March 13,1987.

Parsons, H.M. "An Overview of Human Factors in Robotics," *AUTOFACT 1986,* Nov. 12-14, 1986, pp. 3-11 - 3-17.

Pearson, G.W. "Robotic System Safety Issues—Best Considered in Design Phase," *Occupational Health & Safety,* pp. 38-41, Sept. 1984.

Percival, N. "Safety Aspects of Robots and Flexible Manufacturing Systems," *Proc. 1st International Human Factors in Manufacturing,* pp. 179-183, April 3-5,1984.

Prien, E.P. and W.W. Ronan. *Perspectives on the Measurement of Human Performance* , Meredith Corp., 1975.

*Proposed American National Standard for Industrial Robots and Robot Systems,* Robotic Industries Association, Dearborn, Mich., 1986.

Rahimi, M. "System Safety Approach to Robot Safety," *Proc. of the Human Factors Society - 28th Annual Meeting,* Oct. 22-26, pp. 102-106.

Ramachandran, V. and S. Vajpayee. "Safety in Robotic Installations,"*Robotics and Computer Integrated Manufacturing,* Vol.3 No.3 pp.301-309, 1987.

Ramirez, C.A. "Robotic Intelligent Safety System," *Robots 8,* pp. 19, 50, 62; 1984.

*Request for Assistance in Preventing the Injury of Workers by Robots* DHNS (NIOSH) Publication No. 85-103, Dec. 1984.

*Robotic Assessment Test Sets: Levels 1,2,&3.* SS-GSFC-0029, NASA/Goddard Space Flight Center, Greenbelt, MD.

Simmons, R.G. The Use of Qualitative and Quantitative Simulations, *Proc. AAAI-83,* pp. 364-368.

# 5.0 NASREM TELEROBOT CONTROL SYSTEM: An Architectural Perspective on Safety

Dr. Michael W. Walker
Mr. Dong-Min Kim

Robot Systems Division
Department of Electrical Engineering
and Computer Science
University of Michigan

## 5.1 INTRODUCTION

The applications of robots are many and varied. A primary goal in industry has always been to relieve the human of hazardous tasks. It therefore seems ironic that the use of a robot can create new safety problems.[1,2] Many of our concepts of safety and safety systems[3-6] have evolved from collections of good ideas that have worked at some place and in some time. Usually, they have resulted from investigations into recent significant injuries. In fact, an important part of any safety program is a plan for the investigation of accidents.[7,8] These plans usually include gathering the facts about the accident, analyzing the facts, developing conclusions, reporting the situation, and making recommendations.

One of the results of accident investigation is the collection of data about the most common types of accidents. For example, Table 5-1 shows statistics from a recent survey of accidents involving robots.[9,10]

**Table 5-1. Selected Results of Survey on Causes of Accidents.**

| Cause | Percent |
|---|---|
| Erroneous action of robot in normal operation | 5.6 |
| Erroneous action of peripheral equipment in normal operation | 5.6 |
| Careless approach to robot by human | 11.2 |
| Erroneous action by human in teaching and test operation | 16.6 |
| Erroneous action during manual operation | 16.6 |
| Erroneous action during checking regulation and repair | 16.6 |

The authors of the survey report drew several interesting conclusions.

- A high percentage of accidents occur when robots are manually operated.

This is a common conclusion and results from the fact that the operator is usually physically close to the robot when it is being operated manually. Most industrial robots have two modes of operation: normal and training. In the normal mode of operation the robot is performing a sequence of operations that has been programmed by the operator. The robot runs unattended and there is little or no danger to the operator. The training mode is used to determine the sequences of operations to perform. One of the time-consuming parts of this task is determining the desired sequences of positions of the end-effector. These positions can be very precise and often call for close visual inspection by the operator. After a significant period of time the operator usually becomes accustomed to the robot and becomes unconcerned with the hazards of coming within its reach. Accidents occur when the robot makes an unexpected motion, because of either erroneous action or erroneous commands. For this reason the use of a dead-man switch during training is an important safety feature.[9]

- The dangers arising during automatic operation of robots occur at a rate remarkably higher than that of other automatic machines.

One reason for this is the relatively large working space of the robot. The workspace of most automated equipment can be easily visualized. However, the workspace of a robot is not so easy to visualize. One could stand behind a working robot, unaware of being within its reach.[11] For this reason pinch points are important safety problem with robots. These are positions where an operator could be caught between the robot and another object. Paradoxically, the other object is often a safety barrier.

This brings up the safety aspect of the type of motion control implemented by the robot. In position control, it can be shown that the stiffness of the end-effector is linearly proportional to the position error gain used by the controller. This gain is set as high as possible to reduce the effects of disturbances on tracking ability. These disturbances can be of several forms, from friction and backlash to nonlinear coupling in the dynamics of the manipulator. Unfortunately, another type of disturbance could be the operator's body.

- The operator may be struck by the robot.

This leads to a kinetic energy model for accident analysis,[9] which assumes that injuries result from the body absorbing energy during impacts. By limiting the energy content of the robot, one could limit the amount of energy absorbed by the body during impact and, hence, reduce the risk of serious injury. The energy contained in the robot can be reduced by reducing the mass of the arm, changing its geometrical shape, or reducing its maximum allowable velocity. Reducing the arm's maximum velocity is the most effective method and is commonly used on industrial robots during the training mode of operation.

- Malfunctions accounted for about half of the dangers of robots.

It therefore seems appropriate to strive for some measure of intrinsic safety in the design of the FTS control architecture. The FTS has adopted a control architecture called NASREM: NASA/NBS Standard Reference Model for Telerobot Control System Architecture.[12] This model specifies guidelines for the planning of activities, the organization of information and communication within the FTS controller. In other words, it gives us a model of the robot's world with which we can design and evaluate safety systems.[13] However, although the reference model clearly indicates the importance of safety, it only briefly mentions the role of a safety system. This paper presents a notion of safety in terms of the operation of a NASREM type of controller. The objectives are to characterize the function of a safety system, to identify which features of the existing NASREM architecture could be used as part of it, and to specify what additional features are needed for implementation.

The next section describes the main features of the NASREM architecture. This is followed by a description of the implications of a safety system within NASREM. Then some concepts are proposed for defining safety systems. The final section summarizes the chapter and draws some conclusions from the study.

## 5.2 THE NASREM ARCHITECTURE

The NASREM architecture is a hierarchical control system (Figure 5-1). The system consists of an operator interface from which commands can be entered and state information can be displayed, a global memory in which state and modeling information is stored, and a hierarchy of control levels. There are six levels, which can be described as follows. The inputs and outputs are specific examples drawn from a satellite servicing task for the FTS.

Level 6—Operations Control Level

*Inputs:* commands to schedule the servicing of satellites.
*Outputs:* commands to the service bay manager.

Level 5—Service Bay Control Level

*Inputs:* commands to a service bay manager to perform operations on specific spacecraft.
*Outputs:* object task commands.

Level 4 —Object/Task Level

*Inputs:* tasks to be performed on objects in the workspace.
*Outputs:* keyframe poses (E-moves).

Level 3—Elemental Move

*Inputs:* sequences of keyframe poses (E-moves).
*Outputs:* trajectories of intermediate poses that move the mechanism from one keyframe pose to the next, while avoiding singularities and collisions.

Level 2 —Primitive Level

*Inputs:* collision free trajectories defined as sequences of knot points.
*Outputs*: interpolated desired positions, velocities, and accelerations at evenly spaced points in time.

Level 1—Servo/Coordinate Transfer

*Inputs:* command positions and orientations of manipulators, grippers, and other mechanisms.
*Outputs:* electrical voltages or currents to actuators.

At the lowest level, Level 1, tasks are commands to physical devices, such as D/A converters. As one moves up the hierarchy, the commands become less specific and more mission oriented.

Each level of the control hierarchy includes three systems: sensory processing, world modeling, and task decomposition. The sensory processing system is used to sense physical processes in the FTS system. The world model uses this information to estimate the state of the system and to predict future states. Also, the world model is used to evaluate plans which are produced by the task decomposition system. The evaluation of plans is an obvious feature of the NASREM architecture which should be part of the safety system. This will be discussed in more detail in the following sections.

The operation of the task decomposition system at each level is characterized by an H-module as illustrated in Figure 5-2. These modules convert higher level task descriptions into sequences of lower level subtasks. Thus, the operation of the controller is basically defined in terms of the operation of the task decomposition system, or H-modules. Each H-module has three components: the Job Assignment, JA, which partitions the input task command into distinct jobs to be performed by physically distinct mechanisms; Planners, PL, which convert each job created by JA into a sequence of subtasks; and the Executors, EX, which carry out the subtasks created by the planners.

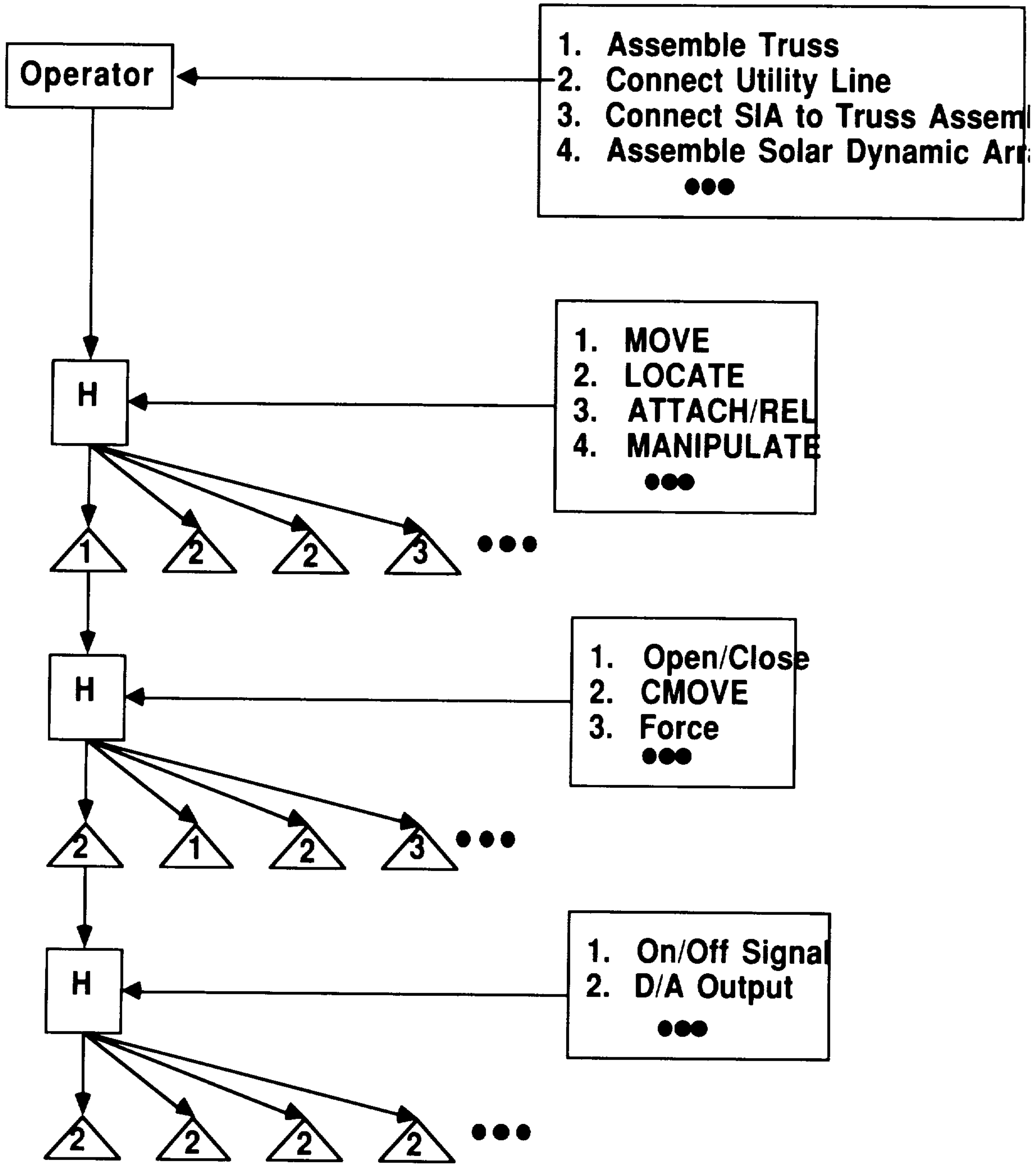
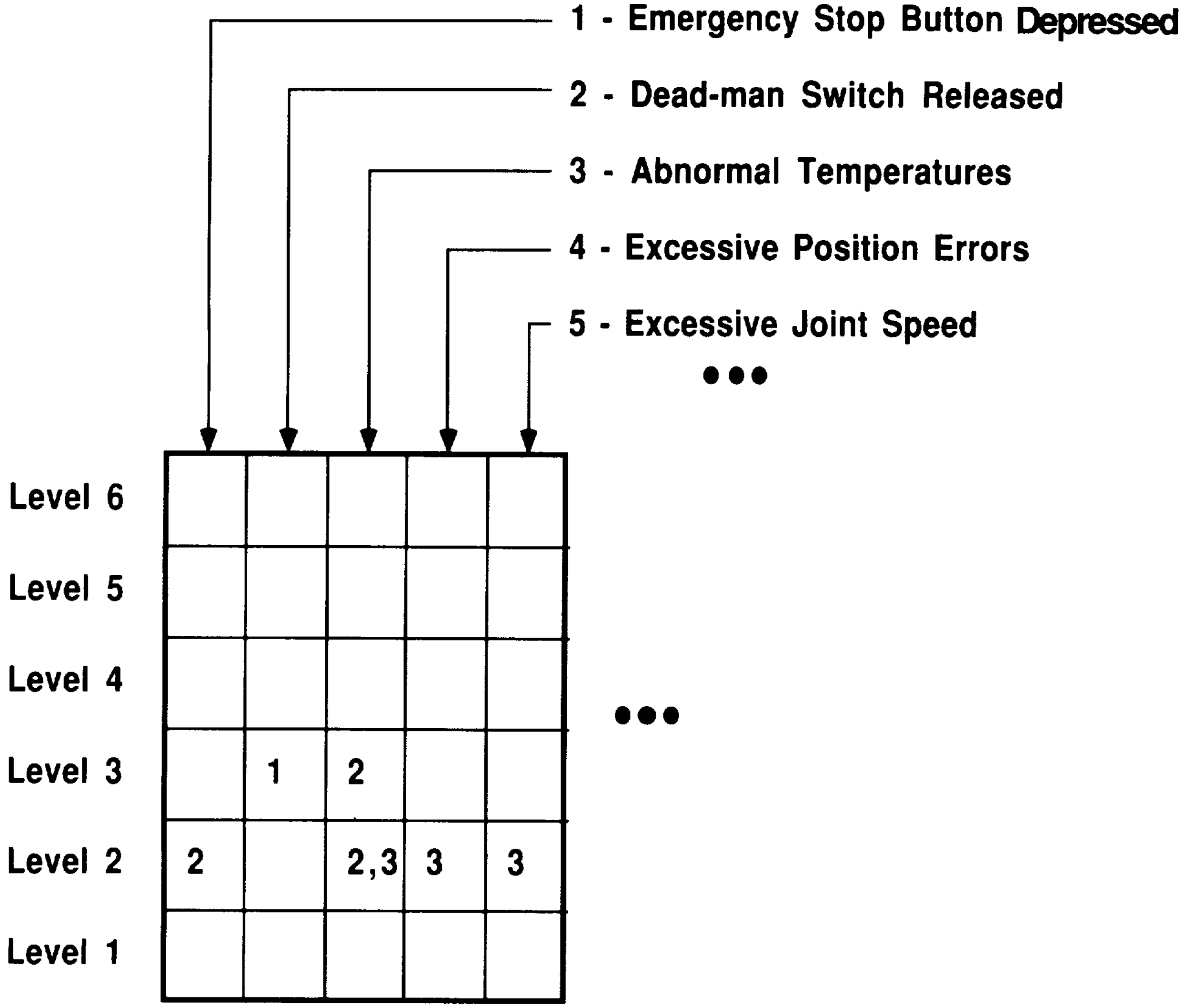


Figure 5-1. NASREM architecture.


1 - Emergency Stop Button Depressed
2 - Dead-man Switch Released
3 - Abnormal Temperatures
4 - Excessive Position Errors
5 - Excessive Joint Speed
●●●
●●●

| | | | | | |
|---|---|---|---|---|---|
| Level 6 | | | | | |
| Level 5 | | | | | |
| Level 4 | | | | | |
| Level 3 | | 1 | 2 | | |
| Level 2 | 2 | | 2,3 | 3 | 3 |
| Level 1 | | | | | |

Figure 5-2. H-module characterizing operation of the task decomposition system at each level.

## 5.3 IMPLICATIONS OF SAFETY ON THE NASREM ARCHITECTURE

The NASREM architecture implies two important safety needs: mechanisms for recovery from hazardous conditions and the ability to convey this information to the operator. There are two aspects of recovery, the recovery from immediate hazards and the avoidance of future hazards. When a immediate hazard is detected, the system must do something to contend with it.

A characteristic of the NASREM architecture is the different planning horizon at each level of the hierarchy (Figure 5-3). The world modeling system is used to evaluate the plans as they are being produced. However, when anomalies occur, these plans must be reevaluated. For example, suppose the sensory system detects an unexpected object in the path of an operating robot, requiring reevaluation of the plan of motion. What should the controller do if the path plan shows that the manipulator will collide with the object? This collision path is, hopefully, ahead in time of the actual robot but probably behind in terms of planning. The controller has several options. It could back up the planners in time to the point where the collision occurs, create a new plan that avoids the object, and return to the old plan at the point where the object is avoided. Or the controller can delete all plans after the time when the collision is predicted and ask the operator for help in handling the problem. The operator would then formulate a new task description to either remove the object or avoid collision with it.

The last major implication of safety in NASREM is communication with the operator. The NASREM architecture lets the operator interact with the system at any level in the control hierarchy and retrieve all state information about the controller. When anomalies occur, the operator must have not only information characterizing the type of anomaly, but also its point in time in the planning sequence. In other words, the operator must know which portion of the task the robot is executing at the time of the anomaly. The problem is how to present this information most effectively, so the operator can best initiate contingency plans.

## 5.4 CONCEPTS FOR IMPLEMENTING SAFETY SYSTEMS WITHIN NASREM

The safety system within NASREM has three parts: anomaly detection, anomaly mapping, and contingency planning. Anomaly detection and mapping are used to identify hazardous conditions. In the operation of NASREM, a hazard does not exist unless an anomaly is detected (anomaly detection) and can be shown to affect current or future plans created by the system (anomaly mapping). NASREM uses contingency planning to recover from hazards.

### 5.4.1 Anomaly Detection

Anomaly detection is the detection of an unexpected event, such as power loss, pressure loss, or an unexpected object in the environment. The premise is that there are a finite number of possible anomalies, each of which can be detected with an appropriate sensor and world modeling system. Each anomaly is assigned a number. A boolean variable, $x_i$ , denotes whether the anomaly has occurred or not. If $x_i$ is true, the i-th anomaly has occurred If $x_i$ is false, the i-th anomaly has not occurred.

Thus, one function of the safety system is to continuously interpret information received from the world modeling system to determine if an anomaly has occurred and to set the associated $x_i$ variable to its correct value. These variables would be used for signaling anomalous behavior, which will effect the current operation of the FTS, andd also the evaluation functions in planning future operations. If a failure has occurred, the $x_i$ variables can be used to plan around it.

### 5.4.2 Anomaly Mapping

Once an anomaly has occurred, the safety system must interpret its effect on the operation of FTS and take appropriate action. The NASREM architecture's framework permits definition of the effects of anomalies on the operation of FTS. Figures 5-2 and 5-3 show that an anomaly makes a set of subtasks in each H-module unexecutable. An example is failure of a D/A converter. This would prevent execution of the subtask in Level 1 that uses the D/A. Another example is the detection of an unexpected object,[14] which could make one of the subtasks at Level 3 unexecutable.

In this way the detection of an anomaly initiates a revaluation of the subtask planned at each level in the control hierarchy. This association of anomalies with subtasks is referred to as anomaly mapping (Figure 5-4).

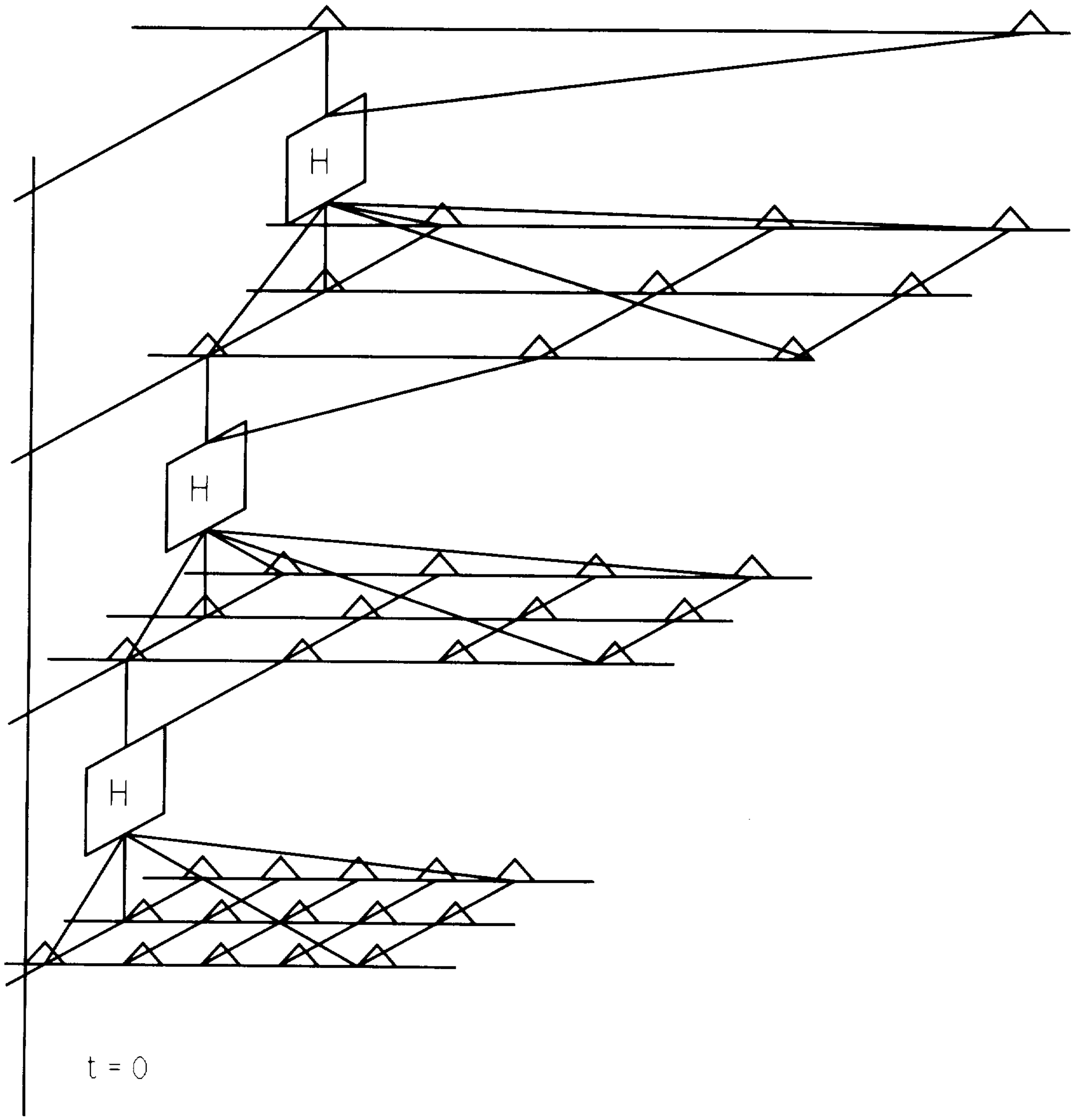


Figure 5-3. Planning horizons for levels of the NASREM architecture.

### 5.4.3 Contingency Planning

When an anomaly has occurred, there must be a plan for contending with it. As described above, the anomaly will be mapped into preplanned subtasks by the anomaly mapper. If no preplanned subtasks are affected by the anomaly, the FTS continues to operate as before. This assumes that the anomaly signals will be used by the evaluation functions during the evaluation of plans. This automatically eliminates from all future plans any anomaly that identifies a particular subtask as hazardous.

If a preplanned subtask is affected by the anomaly, the FTS system must have a new plan. If the subtask is far enough out in time, the controller may be able to simply reset the planning process and resume operation. The creation of a new plan will necessarily avoid the use of the affected subtask, since the associated anomaly variable will still be true. If the subtask is the currently executing task, then another immediate plan would need to be initiated. An example would be a plan to immediately bring the system to a HALT state. The operator would then be queried for a new plan to avoid the hazard.

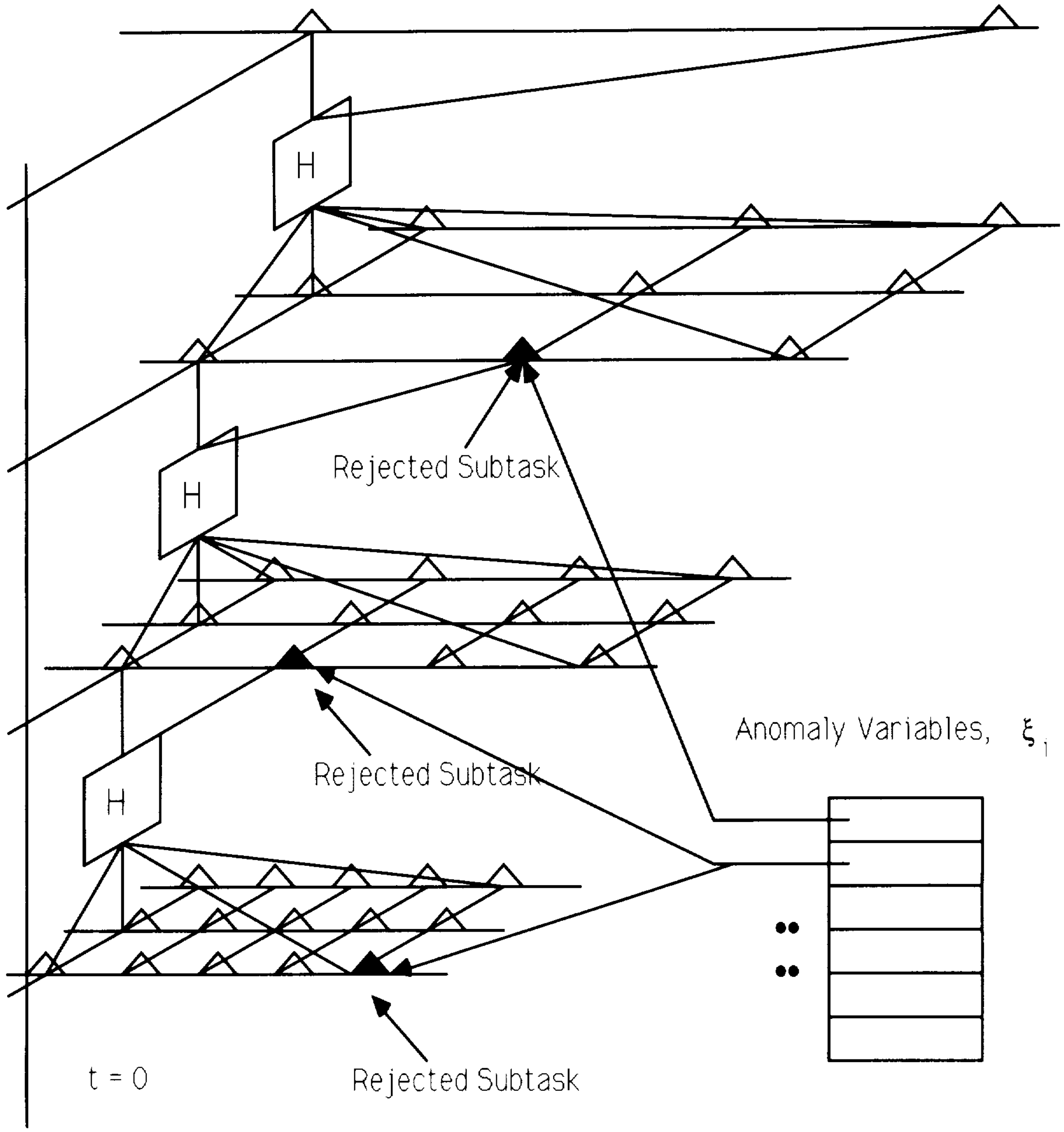


Figure 5-4. Anomaly mapping.

## 5.5 AN EXAMPLE HAZARD SCENARIO

The following example hazard scenario illustrates the concepts just developed. The telerobot has experienced a failure during a Space Station assembly task involving the connection of power utility lines.

A description of a typical operation of the FTS is followed by description of the anomaly detectors required to recognize the anomalies. Then we define the anomaly mappers and illustrate their operation. Finally, we discuss possible contingency plans for hazards.

### 5.5.1 Task Decomposition

The starting point of the following example task decomposition in NASREM is the NASA Robotic Assessment Test Set (RATS) document.[15] It describes the decomposition of a representative set of Level 4 tasks into Level 3 tasks, and on into Levels 2 and 1.

#### 5.5.1.2 Level 3 (E-Move Level) Decomposition

The outputs of the Level 4 are inputs to Level 3. Each command is then decomposed into a Level 2 command. For example, a set of Level 3 outputs might be:

1. Open/Close - Open and close gripper
2. CMOVE - Move to Cartesian Position
3. Force - Apply specified force/torque

Each Level 3 input command would be decomposed into a sequence of these subcommands. As part of the plan evaluation, they would be checked to guarantee freedom from collisions.

#### 5.5.1.3 Level 2 (Primitive Level) Decomposition

The outputs of Level 2 are inputs to Level 1. Each command is then decomposed into a Level 1 command. For example, a set of Level 2 outputs might be:

1. On/Off - Signal to open and close the gripper.
2. D/A Output - Voltage to apply to motor.

Each Level 2 input command would be decomposed into a sequence of these subcommands.

### 5.5.2 Anomaly Detectors

Anomaly detectors come in a variety of forms, for example:[14,16]

1. Emergency Stop Button Depressed
2. Dead-man Switch Released
3. Abnormal Temperatures
4. Excessive Position Errors
5. Excessive Joint Speed
6. Excessive Joint Acceleration
7. Excessive Motor Currents
8. Abnormal Pneumatic Pressures
9. Power Line Surge
10. Power Line drop-out
11. Work Space Intrusion Alarm
12. Data Errors
13. CPU Errors
14. Memory Errors
15. Function Time-outs

Each of these anomalies could be detected by hardware specifically designed for that purpose.

### 5.5.3 Anomaly Mapping

After detection, the anomalies are mapped into subtasks. One method of implementation is to start with a simple table look-up, the rows of the table corresponding to the different anomalies. The table would have n columns corresponding to the n levels of NASREM that are implemented. The intersections of the rows and columns list all possible tasks that might create a hazard if executed. Each task that is flagged as hazardous at one level implicitly identifies all higher level tasks that generated it. In this way only the tasks at the lowest level are identified as hazardous. This identification will automatically filter up to the higher levels, since the Function Time-out anomaly (#15) will notify the Executor components of the H-modules that the lower level tasks are not being completed.

### 5.5.4 Contingency Planning

Contingency planning depends upon the goals of the recovery process. For example, activation of the Work Space Intrusion Alarm (Anomaly #11) signals a revaluation of the planned manipulator motion (subtask #1 of Level 3). Suppose that Sequence #2 (MOVE - Move line to coupler) in the example plan for connecting the utility line produces a collision. The goal in this case might be creation of a new plan to avoid collision, by replacing Sequence #2 with several other subtasks. Examples, in their order of complexity, are:

- a sequence of subtasks that remove the object
- a single new MOVE subtask that avoids the object
- a sequence of subtasks that brings the robot to a HALTed state

In an initial version of FTS, the contingency plan might be the last one listed above. In the HALTed state the robot would simply wait for new commands to be entered by the operator. Although it is not very robust, this method does address the issues of contingency planning in a straightforward and verifiable manner. A desired HALT state and a plan for getting there must be specified for every possible subtask implemented by the system. The system could be tested by creating an anomaly during the execution of a particular subtask, then checking to see if the system achieves the desired HALT.

## 5.6 CONCLUSION

The issues of safety from an architectural perspective have been addressed for the NASREM telerobot control system. The conclusion is that NASREM already has most of the mechanisms required for implementing an intrinsic safety system. This implementation can be achieved by carefully specifying the operation of the planning mechanism during hazardous conditions. In the proposed implementation of a safety system, a hazardous condition is recognized through the use of anomaly detectors and anomaly mappers. The function of these mechanisms is two-fold: 1) to identify which subtasks are hazardous, and hence unexecutable, and 2) to use in the evaluation of future plans. When a preplanned task has been identified as hazardous the planning mechanism is used to produce a contingency plan, such as bringing the operation of the associated devices to a HALT state.

Verification of the safety system could be achieved first by testing a specified set of the anomaly detectors. A second test would show whether the robot achieves the desired HALT state for any possible anomaly occurring during the execution of each subtask.

## 5.7 REFERENCES

1. Potter, R. D. "Safety for Robotics," *Professional Safety*, Dec. 1983, pp. 18-21.
2. Miller, R.K. *Industrial Robot Handbook*, Prentice-Hall, 1987.
3. Earnest, R.E. "Safety Performance Analysis," *Professional Safety*, April 1983, pp. 21-46.
4. Harner, R.E. "*Safety Review: A System of Program Development and Evaluation,*" *Professional Safety*, Oct. 1982, pp. 27-29.
5. Ibasco, M.P. "Step Up Safety Objectives: Keep Up Results," *Professional Safety*, Oct. 1980, pp. 39-42.
6. Griffen, K. G. "Safety for Industrial Robotic Applications," *Professional Safety*, Dec. 1983, pp. 22-26.

7. Ferry, T.S. "Accident Investigation and Analysis," *Professional Safety*, January, 1981, pp. 18-22.
8. Warnecke, H.J. and R.D. Schraft. *Industrial Robots: Application Experience*, I.F.S. Publications Ltd., 1982.
9. Akeel, H.A. "Intrinsic Robot Safety," *Professional Safety*, Dec. 1983, pp. 27-31.
10. Sugimoto, N. and K. Kawaguchi. "Fault Tree Analysis of Hazards Created by Robots," *Proceedings, 13th International Symposium on Industrial Robots.* April 1983.
11. Stowe, W. W. "Robots—Safe or Hazardous?" *Professional Safety*, Dec. 1983, pp. 32-35.
12. Albus, J.S., H.G. McCain, and R. Lumia. "NASA/NBS Standard Reference Model for Telerobot Control System Architecture (NASREM), National Bureau of Standards, Robot Systems Division, March 13, 1987, NASA:SS-GSFC-0027.
13. Capps, J.H. "Systems Concepts for Safety Progress," *Professional Safety*, March 1980, pp. 41-45.
14. Meagher, J., S. Derby, and J. Graham. "Robot Safety/Collision Avoidance," *Professional Safety*, Dec, 1983, pp. 14-16.
15. *Robotic Assessment Test Sets: Levels 1, 2, & 3*, NASA:SS-GSFC-0029.
16. Lauch, K.E. "Safeguarding Industrial Robots," *National Safety News*, April 1984.

## BIBLIOGRAPHY

Lodge, J.E. "How to Protect Robot Maintenance Workers," *National Safety News*, June 1984.

National Safety Council Data Sheet I-717-85, *National Safety and Health News*, Oct. 1985.

Percival, N. "Is Robot Technology Safe?" *Decade of Robotics*, 1983.

Rosenthal, H. B. "Safety Analysis and Review System," *Professional Safety*, Feb. 1982, pp. 15-20.

Russell, J. W. "Robot Safety Considerations," *Professional Safety*, Dec. 1983, pp. 36-37.

Salim, P. "The Robots Are Coming, " *Professional Safety*, March 1983.

Stonecipher, K. *Industrial Robotics*, Hayden Book Company, 1985.

Ziskovsky, J.P. "Risk Analysis and the R3 Factor," *Robot 8 Conference Proceedings*, vol. 2, 1984, sect. 15, pp. 9-21.

# 6.0 SOFTWARE SAFETY FOR THE FTS

Dr. Kai-Hsiung Chang
Dr. James Cross
Mr. Steve Dannelly

Department of Computer Science and Engineering
Auburn University

## 6.1 INTRODUCTION

NASA has committed to the design and implementation of a Space Station Flight Telerobotic Servicer (FTS) to assist the astronauts in assembly, maintenance, servicing, and inspection tasks on the Space Station and the Space Shuttle.[1] FTS has three unique characteristics:

1. It will be required to operate in a much less structured environment than current industrial robots.
2. Most planned actions cannot be tested except at execution.
3. There is little repetition in its actions. Furthermore, the FTS is required to grow and evolve with time.

One of the major requirements of FTS is safety. An acceptable level of safety can only be reached by analyzing and implementing safety issues through its conceptualization, design, construction, and operation phases. This safety requirement is not solely dependent on the visible hardware components such as manipulators and hydraulic systems. It is also dependent on the underlying software that controls every action of these hardware components. In order to achieve maximum safety, software safety must be considered. Software safety is defined here as a requirement that the software system be reliable and fault-tolerant. That is, it performs its tasks with a minimum of errors, and can detect, predict, and recover from hardware and software errors or failures.

Although safety issues have been studied since the early stages of robotics applications, emphasis has been placed on the hardware configuration design and mechanical guarding systems. Software safety is rarely mentioned. However, there is an increasing consensus on the importance of software safety.[2]

The objective of this chapter is to identify issues that need to be addressed in considering software safety and to summarize state-of-the-art approaches to software safety. Three issues are critical in achieving this.

**Software Design Philosophy.** This identifies fundamental design requirements for every software package or system in the FTS. Among these requirements, software validation and verification (V&V) ensures that a software package has been designed according to its specifications and has been correctly implemented at the code level. Other requirements might involve the accessibility of internal software status, backup system for failure, and error recovery. Also considered is AI software, whose basic structure differs from that of conventional software. Well-established conventional V&V methods may not be applicable to AI software development, though the problem has never been fully addressed. However, several promising approaches for AI software V&V have been proposed recently, and these may give a direction for future AI software development.

**Operating Modes and Warning Levels.** Different operating modes such as programming, manual, and execution, should provide different levels of FTS action constraints and safety sensitivity. When a safety violation is detected, the software system should reason about the degree of seriousness, based on the operation mode and the type of violation, so that appropriate actions can be taken.

**Safety Subsystem Software (Watchdog).** A separate safety subsystem (also known as Watchdog) can provide more reliable software performance. Watchdog is responsible for monitoring both software and hardware functions of the FTS. For software monitoring, Watchdog can check the consistency of information from redundant sources and/or the correctness of information by graphic simulation or other methods. Hardware function monitoring needs status information from sensory systems. The Watchdog software must first analyze the information and determine the existence of failure and violation. When any of these conditions exist, impact/damage analysis is required before appropriate actions can be taken.

In order to accomplish the items listed above, cooperation with other disciplines will be needed. For example, the software design philosophy must be incorporated throughout the conceptualization, design, and implementation phases. A safety subsystem can function fully only if the sensors on which it depends are known to work properly and if the system is aware of the sensors' limitations.[3]

## 6.2 SOFTWARE DESIGN PHILOSOPHY

Traditional software engineering principles are expected to form a strong basis for FTS software development.[4] From a safety standpoint, validation and verification are perhaps the most critical issues in the development of safe software.

Validation refers to activities that ensure the software meets the customer's reasonable expectations, that is, what was intended, as opposed to what was written. Verification refers to activities that ensure the software corresponds to a written description. For example, verification occurs when the source code is shown to accurately reflect the detailed design specification.[5,6] Various groups, such as NASA and DOD, have their own requirements for V&V.[7] These usually include many varying aspects of software engineering.

**Software testing** is a major part of V&V. Testing is a set of activities that can be planned in advance and conducted systematically throughout the software life cycle. The following briefly describes four general testing steps that correspond directly to the software engineering stages of code, design, requirements, and system engineering.[6]

1. *Unit testing,* which focuses on the smallest unit of software design—the module. It assures the integrity of such things as local data structures, interfaces, and error-handling paths.
2. *Integration testing,* which tests whether the modules fit together as they should. This is usually performed in a bottom-up manner, beginning with the atomic modules and adding them together until the program has been constructed.
3. *Validation testing,* which is done after the software has been assembled. Here the package is examined to see if it is in accordance with the customer's expectations.
4. *System testing,* done after the software is added to the larger system of hardware and information. It includes recovery testing, stress testing, and performance testing.

Software testing must be done at every phase of building software. Errors should be caught early and removed so that they do not cause further errors. However, testing alone does not assure quality software.

**Software Quality Assurance.** Since quality must be incorporated throughout the software engineering process, much of V&V encompasses what is known as software quality assurance (SQA).[6] This is yet another very broad area that can only be briefly mentioned. SQA involves such things as analysis and design methods and tools, formal technical reviews, testing strategies, control of documentation and changes made to it, development standards, and mechanisms for reporting and measuring quality.

**MSFC software engineering guidelines.** These guidelines[7] refer to V&V in two ways. First, as particular phases of the development life-cycle, and second, as an ongoing process in concurrence with the life-cycle. The reference document describes the typical life-cycle as the following sequence of phases: 1) Conceptual, 2) Requirements, 3) Design, 4) Code and Debug, 5) Verification, 6) Validation, 7) Systems Integration, and 8) Operations and Maintenance. The verification phase is to test logic paths, operating modes, and failure modes against the Software Requirements Specification. In the validation phase emphasis is on system integration testing.

**V&V as a Management Tool.** V&V is also a management tool, which supplements SQA to ensure an orderly process of software development. Here, V&V is divided into three phases which cover every step of the life-cycle. Phase I, which covers step 1, consists of requirement analysis and test planning. Phase II, covering steps 3 and 4, is made up of equation and design analysis and facility development. Phase III, covering steps 5, 6, 7, and 8, consists of coding analysis and testing.[7]

Currently, software engineering researchers are working on automated and semi-automated tools and methodologies. An effective methodology can assist a designer with respect to both the design itself and its verification.[8] There are also tools which help the software engineer to automatically verify code in a number of different ways. Errors are much less likely to arise in a system that was developed by another system that has been verified.

**Artificial Intelligence Software.** Another V&V aspect to be considered is artificial intelligence (AI) software, especially rule-based systems. Although AI software has been widely used in many applications, its V&V methodology has not been fully addressed. This has become a major stumbling block to extended use of expert systems. As stated in Culbert et al.,[9] there exists a vicious circle in expert system V&V: V&V of expert systems is not done because nobody requires it. Nobody requires V&V of expert systems because nobody knows how it can be accomplished. This cycle must be broken for expert systems to succeed.

In a recent paper, O'Keefe et al.[10] state some useful guidelines for validating expert systems:

1. We must validate systems only against an acceptable performance range for a prescribed input domain. Previous human performance indicates the acceptable range.
2. We should build validation into the development cycle. Often, we must carry out a cross-sectional performance validation prior to implementation, and specific validation tests as the system evolves after implementation.
3. We must choose an appropriate qualitative method: Field-testing may be acceptable for noncritical applications. Turing tests are useful for comparing systems against experts in blinded evaluations, and can avoid pro- or anti-computer bias. Subsystem validation and sensitivity analysis are useful for validating specific areas of concern.
4. We must use quantitative methods where applicable, and as informatively as possible, for instance, to produce confidence intervals rather than single-point estimates. We must be aware of the multiple-response problem, and use appropriate multivariate techniques.

Three specific approaches to the V&V of rule-based expert systems have been reported. In the approach described by Culbert et al.,[9,11] if proper techniques are used to document requirements, V&V of rule-based expert systems is possible and may be easier than with conventional code. A common characteristic of expert system development is that relatively few requirements are initially specified. Typically, a rather vague, very general requirement is suggested, for instance, "We want a program to do just what Charlie does." Solid requirements written down in a clear, understandable, easy to test manner generally don't exist. This is why most expert systems are difficult to verify and validate—not because they are implicitly different from other computer applications, but because they are commonly developed in a manner which makes them impossible to test!

Therefore, the obvious solution is to use a methodology which will produce written requirements. These can be referred to throughout development to verify correctness of approach. Also they can be tested at the end of development to validate the final program. An alternate approach would be to write most of the requirements and specification documentation after completion of the prototyping phase. In essence, the prototype would form the basis for the requirements and would act as a "living spec."

Along with a requirements document a test plan should be written. The test plan should describe how the requirements and/or prototype will be checked for completeness, consistency, feasibility, maintainability and testability.

Finally, the requirements must be examined to ensure that they can be tested. An advantage of expert systems is that the system requirements and the rules of problem solving can be coded directly in very high level descriptions. This makes the requirements and rules examination very simple. The examination can be performed by a panel consisting of experts, developers, and managers to ensure adequate coverage of all areas of concern.

A second V&V approach for rule-based expert systems was proposed by St. Clair et al.[12] Their approach suggests comparing the output set (E) of an expert system with a known set of correct conclusions (C) for a given set of input data and make decisions on how to refine the rule base. Each system output conclusion can be classified into one of the following cases: 1) Correct conclusions, or E $\cap$ C, 2) Incorrect conclusions caused by incomplete or incorrect rules, or E - C, 3) Incorrect conclusions caused by incorrect or missing rules, or C - E. After a conclusion classification is made, appropriate steps can be taken to fix the rules that were involved in the rule chaining.

The final approach was proposed by Fernandez and Hinman.[13] There, a hierarchical structure was developed for an On-Orbit Tele-Robotic system. In order to verify the decisions (or plans) from the AI software, they used computer graphic simulation. A three-dimensional solid model is built for the work space which is similar to the 3-D simulation of a later section. The simulation will verify that: (1) the planned robot path is correct for the task; (2) the inverse kinematic equation may be solved at all points along the program (controllability); and (3) the arm or other components will not collide accidentally with obstacles within the workcell. This key idea is to provide a chance of rehearsal on a computer graphic simulator, which will also allow human operators to anticipate problems that may occur.

Other aspects of AI software verification may involve software components such as a knowledge base and an inference engine.[9] For a knowledge base, items to be checked include correctness, completeness and consistency. For an inference engine, rule-matching, conflict resolution, and information updating should be verified. Very limited literature can be found on this area.

Testing through simulation remains the most effective method available for final validation. However, for any system of reasonable complexity, exhaustive testing is both prohibitively expensive and time consuming. Space Shuttle applications typically used extensive testing with data sets representative of the anticipated problems or failure modes.[9] This method is not guaranteed to eliminate all software bugs, but it can prevent the anticipated problems.

## 6.3 OPERATING MODES AND WARNING LEVELS

The FTS will need to be operated in different modes. Each mode determines the allowable conditions and defines system integrity checks. Software subroutines provide control over the mode of the FTS.[14] Following are some of the operating modes.

**Teaching Mode.** The robot learns to perform certain actions by being taught manually, either from a remote console or by an EVA astronaut. The safety subsystem must be used to monitor all actions. If an astronaut is close to the robot, restraints such as speed limits on control joints should be applied.

**Execution Mode.** The manipulator is performing planned actions in "full speed." All monitoring and real-time simulation subsystems should be functioning.

**Programming/Planning Mode**. The action plan of the FTS is generated through numerical computation and/or artificial intelligence reasoning processes. In some cases, programming/planning mode is not allowed to coexist with execution mode. Under these circumstances, all manipulator actions should be frozen and the safety subsystem may be shut down for maintenance. However, if programming/planning and execution are allowed to coexist, the safety subsystem should do its work as well. After an action plan has been generated, an action simulation can be used to verify the correctness of the plan.

**Manual Mode.** It is important to provide an operating mode that allows direct or manual control of most control joints of the manipulator and the robot. This mode is necessary when software errors prevent access of control joints. During direct manual operation, all monitoring and simulation subsystems should be functioning and providing warning signals. However, override to any warning should be allowed.

The operating modes just described are also important for other safety reasons. First, different safety violation triggering levels may be required for different modes. For example, during the execution mode when an astronaut is detected within five meters of the manipulator, a warning may be required. However, a warning may not be required until the manipulator is within one meter of an astronaut during the teaching mode.

Second, different responses may be required for safety violations or failures in different operation modes. This requires an analysis and assessment of current operation and status. Uniform responses may not be adequate. For example, if a dangerous piece of equipment comes close to the robot while it is performing an automatic task it may be necessary to freeze the robot's action. Of course, this same reaction is not applicable while in manual mode. The astronauts may be using the robot with the intention of grasping the piece of equipment, and so only a warning is required.

A third safety aspect that is associated with operation modes is the "warning levels."[15] Conventionally, this method divides the surrounding area of a robot station into several zones, for detection of intrusion and several layers of protection against it. The zones are implemented with different types of sensors, so that when an intrusion is detected, appropriate warning signals and reactions can be activated. In the FTS environment, the telerobot is movable. This means dynamic change of the detection zones. Sensor information and simulation can be used to determine the location and the surroundings of the telerobot.[16]

## 6.4 SAFETY SUBSYSTEM SOFTWARE

The safety subsystem, also known as the Watchdog Safety Computer System, would be a stand-alone computer system used to monitor robot-related operations in the FTS. The purpose of this subsystem is to detect software/hardware operations that are outside the range of normal conditions and to stop the robot before a collision or any damage occurs to equipment or astronauts. Watchdog requires one or more separate computers, as well as cooperation with other parts of the FTS system. This includes internal status information about the robot control software, sensory information from joints, intruder detectors, cameras, and other components.

A software structure that would provide this capability has been discussed by Albus et al.[17] Two aspects, software protection and system monitoring and simulation, are described next.

### 6.4.1 Software Protection

Though expensive, redundancy offers a good protection against software failure. A doubly-redundant system can shut itself down when its two components disagree, and a triply-redundant system can use majority vote to override one failed component and continue operation.[4,18]

Time-outs are another simple and effective software failure test.[4] In a multiprocessor control system, one might require regular transmissions between all computers and the Watchdog system. The failure of the Watchdog to receive a transmission on time would indicate a failure in the tested computer.

A status check is a third way to detect software failure.[4] In a status check, one computer sends specific data to a second computer which can tell if the data is self-consistent. A description of what a given piece of software is supposed to do could form the basis of one type of simple status check. For example, the software in a computer controlling a robot arm should at least try to keep each joint position within the physical limits determined by the design of the arm. Therefore, one simple status check would be for that computer to report the current arm joint positions to a second computer, with the second computer determining whether the positions are reasonable. This would require only a little of the second computer's time.

### 6.4.2 System Monitoring and Simulation

The purpose of system monitoring and simulation is to predict, detect, and prevent robot operation errors through analyzing system status. This status information can come from two sources. One is the internal status of the control software—the computer's version of the "world" of the FTS system. The other is information from various sensors, which provides the "actual" status of the FTS system.

Some safety violations, such as intruders and excessive joint movement, can be detected through simple status checks. However, many safety violations and failures can be detected only through complex reasoning and simulation. The following are methods that can be used for violation and/or failure detection.

**Status Verification.** The purpose is to confirm that the control software's version of the "world" is equivalent to the actual world. The robot control software contains the current position and motion information of each joint of the FTS. This information can be obtained through computation or direct sensory feedback. However, software or hardware errors may result in incorrect information. Since the current world status is the basis of all robot operations, this error should be detected as early as possible. There are two ways of achieving this status verification: A second set of sensors can be installed and linked to the Watchdog system. Their status information can be used to verify the readings of the control software. If there is a difference between the control software's status and the Watchdog's status, an error is detected. This approach could be expensive. The other way is using status information from other sensors such as a vision system to determine the current positions of each joint. A geometrical structure analysis may be needed to conclude these positions. This information can then be used to compare with the software's internal status. This method may cost less in hardware, but need more computation, and the result may not be as accurate as the first method.

**Three-Dimensional Solid Model Simulation.** This method, also known as "Forbidden Volume Algorithm," gives the safety subsystem the ability to impose restrictions on the motion of the manipulator and the robot. Each object in the work space is represented as a 3-D volume and is stored in a "world model." The volumes of the robot and the manipulator can be dynamically computed by transforming their physical geometries and joint positions into 3-D space. Any possible collision can be detected when the robot is about to cross the surface boundary of an object's volume. With the volume defined as larger than the object, the robot reaches the surface boundary before colliding with the object. The safety margin can be adjusted by changing the sizes of the object volumes. Surveys of industrial robot accidents show that a major cause of mishaps is "robot-runaway," where the robot overshoots its intended motion. Kilmer and others have defined mathematical formulas for computing forbidden volumes with different levels of risk, depending on robot speed.[19]

Forbidden Volume Algorithm also has other applications. First, it can be used to simulate the "planned" actions before execution. This is important in verifying robot action plans.[13] Second, the physical world can be displayed as 3-D graphs and can be viewed from different angles as desired. This will give the astronauts a clear picture of the work space.[13] Third, since the graphic simulation provides views of different angles, it can also be used to determine if the locations chosen for closed circuit TV cameras will provide an unobstructed view.[13]

## 6.5 CONCLUSIONS AND RECOMMENDATIONS

Software safety will be a key link in the FTS system. Unfortunately, this issue has been rarely mentioned in the current industrial robotic experience. The chapter has identified three areas that are associated with this issue: software design philosophy, software operation modes, and a safety subsystem. Among these findings, most are general safety concepts and will need to be elaborated upon for the final design of the FTS. The following recommendations are included:

**Software Design Philosophy.** Validation and verification techniques must be applied to the development of every software module and system. Much of V&V encompasses what is known as software quality assurance (SQA), which is applied throughout the software engineering process. SQA involves such things as analysis and design methods and tools, formal technical reviews, testing strategies, control of documentation and changes made to it, development standards, and mechanisms for reporting and measuring quality. Among these items, software testing is a major part of V&V. It consists of four steps:

- Unit testing
- Integrating testing
- Validation testing
- System testing

A well-defined software development life-cycle represents an important point in the development standard. A typical life-cycle can be described as the following sequence of phases (with possible iteration): 1) Conceptual Phase, 2) Requirements Phase, 3) Design Phase, 4) Coding and Debugging, 5) Verification, 6) Validation, 7) Systems Integration, and 8) Operations and Maintenance.

Software development tools will also be an important factor in future software implementation. For example, a software tool such as Hamilton Technologies' 001[20] allows the developer to specify software at a much higher level of abstraction than afforded by a typical HHL. For many SQA items, such as project and documentation control, the emphasis may be on the management procedures with semi-automated tool support.

For rule-based AI software, it is recommended that system requirements, design and development details, and test plans be documented. A panel composed of experts and decision makers then examines these documents.

**Software Operation Modes.** It is recommended that the anticipated FTS tasks be analyzed such that various operation modes can be recognized. Some example operating modes are:

- Teaching
- Programming
- Execution
- Manual

Appropriate safety considerations must be adapted for each mode.

**Safety Subsystem Software.** A Watchdog safety subsystem is recommended. Although it may be costly, the Watchdog should cover all safety aspects to the extent possible. Suggested items include software protection, system monitoring, and simulation. Software protection emphasizes software redundancy and time-out checking. System monitoring and simultation require separate hardware and software components. The task of monitoring is performed through status verification which detects any information inconsistency. The task of simulation is done through the 3-D solid model simulation of the world.

## 6.6 FUTURE WORKS FOR SOFTWARE SAFETY

The Auburn University team has identified four areas for future FTS safety studies.

**Selection and Implementation of Software Safety Methods.** The selection and implementation of software verification and validation methods and the design of the Watchdog safety system will depend on the detailed specification and design of the FTS. The suitability and cost-effectiveness of each method must be analyzed and measured based on the detailed FTS design. This analysis and measurement should be performed before the construction of the software and hardware components of the FTS.

**Collision Analysis and Projection.** Although in this study various precautions are suggested for the FTS to avoid collision, certain types of collision may be tolerable. A collision-free FTS can be extremely expensive, due to extensive computation, simulation, and monitoring. There may be environments in the FTS application in which "tangent" collision will not damage any components and task procedures. By allowing such collisions, the FTS performance may be greatly improved. However, the environments and tasks for this type of collison must be identified and carefully analyzed in the FTS design. Before each application of such cases, the collision effect must be calculated to ensure safety.

**System Performance Projection.** Monitoring of major system components (hardware and software) can provide their performance history. A consistent performance trend can be used to set up a maintenance schedule. An inconsistent performance history will suggest a component replacement or readjustment. A knowledge-based system, in which past performance and general rules are stored, could be used to derive this projection. Experience in manufacturing system can provide a useful guideline.

**Intelligent Human-Machine Interface.** Although astronauts have the highest priority in accessing and controlling the FTS, incorrect or unsafe human operations are possible. One way of minimizing this impact is to provide an intelligent human-machine interface. This interface will predict the intent of human operation, based on the operating history and current world model. If the human operation is out of the intelligent interface's prediction scope, a warning will be activated. Acknowledgement from the astronauts is needed to proceed with the operation. However, under certain environments, an override to the interface warning should be allowed to provide quick operation. This intelligent interface will be very important in situations involving multiple users.

## 6.7 REFERENCES

1. Hinbal, S. W., J. F. Andary, J. G. Watzin, and J. E. Provost. "The Flight Telerobotic Servicer (FTS): A Focus for Automation and Robotics on the Space Station," *2nd AIAA/NASA/USAF Symposium on Automation, Robotics, and Advanced Computing for the National Space Program*, March 9-1, 1987.
2. Akeel, H. A. "Intrinsic Robot Safety," *Professional Safety*, Dec. 1983, pp. 27-31.
3. Ramirez, C. A. "Robotic Intelligent Safety System," *Robots 8*,, 1984, pp. 19-50-62.

4. Park, W. T. "Robot Safety Suggestions, " SRI International, Technical Note No. 159, April 29,1978.
5. Howden, W. E. *Functional Program Testing and Analysis*, McGraw-Hill, 1987.
6. Pressman, R. S. *Software Engineering: A Practitioner's Approach*, McGraw-Hill, 1987.
7. *MSFC Software Management and Development Requirements*, (MA-001-006-2E), NASA-Marshall Space Flight Center, AL 35812.
8. Hamilton, M. and S. Zeldin, "The Relationship Between Design and Verification," Higher Order Software Inc., 1979.
9. Culbert, C., G. Riley, and R. Savely. "Approaches to the Verification of Rule-Based Expert Systems," *Proc. Space Operations-Automation and Robotics Conference*, August 1987, pp. 191-196.
10. O'Keefe, R., O. Balci, and E. Smith. "Validating Expert Systems Performance," *IEEE Expert*, Winter 1987, pp. 81-89.
11. Culbert, C., G. Riley, and R. Savely. "Verification Issues for Rule-Based Expert Systems," *Proc. 3rd Conference on Artificial Intelligence for Space Applications*, November 1987, p. 1-7.
12. St. Clair, D., W. Bond, and B. Flachsbart. "Using Output to Evaluate and Refine Rules in Rule-Based Expert Systems," *Proc. 3rd Conference on Artificial Intelligence for Space Applications*, November 1987, pp. 9-14.
13. Fernandez, K., and E. Hinman. "The Use of Computer Graphic Simulation in the Development of On-Orbit Tele-Robotic Systems," *Robots 11*, April 26-30, 1987.
14. Cook, B. A. "Increased Hardware Safety Margin through Software Checking," *Robot Safety*, IFS Publications Ltd.,1985, p. 161.
15. Sneckenberger, J. E. and K. Kittiampon. "Practical Aspects of Safety System Inplementation for Robotic Work Stations," Project Report, Dept. of Mechanical and Aerospace Engineering, West Virginia University, May 15, 1985.
16. Lee, M. H., D. P. Barnes, and N. W. Hardy. "Knowledge Based Error Recovery in Industrial Robots, " *Proc. Eighth IJCAI*, vol.2, pp. 824-826, August 8-12, 1983.
17. Albus, J. S., R. Lumia, and H. McCain, "Software Architecture For Manufacturing and Space Robots," *2nd AIAA/NASA/USAF Symposium on Automation, Robotics, and Advanced Computing for the National Space Program*, March 9-11, 1987.
18. Neese, T., K. Shin, and M. Leu. "High-Level Design of a Spray Finishing Robot Controller," *Robots 11*, April 26-30, 1987.
19.Kilmer, R. D., H. G. McCain, M. Juberts, and S. A. Legowik. "Safety Computer Design and Implementation," *Robot Safety*, IFS Publications Ltd., 1985, p. 141.
20. *HTI001 Users' Manual*, Hamilton Technology Inc., Cambridge, MA.

# 7.0 DESIGNING FOR SAFETY

## 7.1. REQUIREMENTS AND CERTIFICATIONS

Establishing realistic safety requirements and certificating that they are being met are continuous, major efforts. EVA has traditionally required extensive rehearsals for specific tasks. The FTS provides an opportunity to ease the limits and expense of outside operations. Design engineers with access to FTS subsystems can challenge and revise safety requirements during the development of space station rather than having to wait for on orbit confirmations as with the RMS or MSC arm.

A test facility, such as a cage or restraining volume, can be provided on the operational space station. The facility can allow for testing of the FTS from the ground or by an IVA astronaut. Such a facility could also be used to conduct other zero-gravity engineering tests and demonstrations.

## 7.2 ENGINEERING COMMENTS

### Emergency Response

Should the user interface provide an emergency scream response, or other physiological factor, that is speaker independent? The interface might monitor via radio and audio/air channels. The FTS response might be to freeze or slow down. The computer would change over to a data collection and survey mode.

### Emergency Power

There is always a worry that FTS will lose power and not maintain its basic computer and motor responses. This is especially important if the device is located at a distant part of the station. Perhaps FTS should have a small, permanent solar power array and attached battery that could maintain power to the CPU that monitors safety. It could also power critical communication and joint control circuits. FTS should be able to accept emergency backup power from an unfurlable solar array, from a space suit power supply, and perhaps via laser or microwave beam from the station. Conversely, FTS should be able to supply emergency power to a space suit or small equipment located near the extremities of the Space Station.

### Thermal Indicators

The FTS must operate under a greater range of thermal conditions than any other space equipment. Situations may arise in which crew may have to work on an FTS whose parts are at very different temperatures. Telemetry on temperature could be provided from points about the FTS to the workstation. Alternatively, liquid crystal paints or patches that change color with temperature could be placed about the FTS to give direct visual readings. Some patches might change color permanently if critical temperature limits are exceeded.

### Zero-gravity

Zero-gravity conditions in the space station may pose new operational hazards. There will be a nominal level of humidity in the station. Care must be taken when bringing a cold FTS into the pressurized environment. Water will likely form drops throughout the FTS structure and float in zero gravity for long periods. Drops moving under the electric fields of startup conditions could short out power circuits and pose safety hazards to a crew member performing and checking out repairs. Dust generated by internal gears, cutting, welding, or turning screws could also float around inside FTS and then short out power circuits under startup conditions.

## 7.3 NASA DOCUMENTATION

NASA program documentation of space station is not in the direct purview of the Human-Robot Safety group but is of crucial importance to safety. We realize that the Space Station program is still in an early phase of development. However, the early draft documentation available to the group does not emphasize FTS safety. The 1987 Space Station operations task force document[1] deals with safety only at the level of introducing topics into the overall outline. For example, "Safety" is the topic of pages 100-103. No details are provided. We feel that section IV on "Telescience" on page 115 might also be relevant to the development of the FTS as a device capable of active safety roles. Other topics include the need for early, extensive crew involvement in the development of both FTS and related operational procedures. This should start with the design phase so the crew is sufficiently familiar with FTS. Practical matters, such as the release of stored energy, are important to the crew.

The basic document of the Space Station program[2] has a section (6.0) devoted to Crew Safety. However, it does not mention the FTS. There should be a comprehensive review of past manned IVA & EVA repair tasks. Such a review will advance the safety of FTS and its use as an active element in the overall safety of the Space Station.

## 7.4 REFERENCES

1. Space Station Operations Task Force Summary Report. NASA Headquarters, Office of Space Station, October 1987, 128 pp. plus appendices.
2. NASA Space Station Man-Systems Integration Standards, NASA-STD-3000, vol. IV, Baseline December 18, 1986, Johnson Space Center, SL0002883.

# 8.0 FUTURE WORK

## General

Establish a broad, high priority program to identify how the FTS can improve the level of safety in the space station.

Consider opportunities to use FTS to design in higher safety and to accelerate the requirements and certification process for space station.

Examine the automation and robotics reports of the phase B and the phase C/D contractors for opportunities to use FTS to increase space station safety.

Develop scenarios in which the use of FTS provides additional contingent options in both the FEL and the operations phases.

## Presence Detecting Systems

Identify existing and potential systems and examine their applicability in terms of industrial experience and the projected space station environment.

## NASREM

Examine the NASREM architecture and determine how to do anomaly mapping, anomaly detection, and contingency planning within it. Determine the safest techniques for force control and management of end-effector position.

## Software Safety

Define methods for verifying and validating FTS safety software. Develop and demonstrate useful "watch-dog" software.

## FTS Safety Simulator

Develop a computer simulation of robot performance. Use it to study FTS's response to various emergency conditions.

## FTS Mobility

Mobility would increase the FTS' usefulness significantly. At the same time, self mobility leads to many safety and engineering problems. A study of mobility is essential, especially since Johnson Space Center is developing a robot to retrieve EVA astronauts and components that escape the Space Station.

## Human-Machine Interface

A properly designed user interface is important in FTS operations, especially for future expansion. The interface for the FTS needs further study and consideration.

## Autonomy

Autonomy is an important aspect in the evolution of the FTS. Increased autonomy brings about more usefulness, but at the same time raises many problems such as complexity, cost, and reliability. A study of autonomy and its benefits and consequences will determine the level needed for the FTS.